Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Alenka Turk

Protokoli za varno elektronsko pošto

diplomsko delo

univerzitetni študijski program prve stopnje
računalništvo in informatika

Mentor: dr. Andrej Brodnik

Ljubljana 2014

Besedilo je oblikovano z urejevalnikom besedil LaTeX.

Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Tematika naloge:

Elektronska pošta je bila ena prvih storitev, ki se je pojavila na internetu. Tako je bila podobno, kot ostale zgodnje internetne storitve, načrtovana brez kakršnegakoli ozira na varnost pošiljanja. Ena od posledic je, da je zlahka zlorabiti sistem za pošiljanje elektronske pošte v imenu druge osebe.

V diplomski nalogi najprej podrobno preučite arhitekturo sistema za pošiljanje in dostavo elektronske pošte ter v njej poiščite šibke člene. V nadaljevanju preglejte obstoječe protokole, ki omogočajo zaščito pred pošiljanjem pošte v imenu drugega, namestite ustrezno programsko opremo in preverite delovanje.

Izjava o avtorstvu diplomskega dela

Spodaj podpisana Alenka Turk, z vpisno številko **63080155**, sem avtorica diplomskega dela z naslovom:

Protokoli za varno elektronsko pošto

S svojim podpisom zagotavljam, da:

- sem diplomsko delo izdelal samostojno pod mentorstvom dr. Andreja Brodnika,
- so elektronska oblika diplomskega dela, naslov (slov., angl.), povzetek (slov., angl.) ter ključne besede (slov., angl.) identični s tiskano obliko diplomskega dela,
- soglašam z javno objavo elektronske oblike diplomskega dela na svetovnem spletu preko univerzitetnega spletnega arhiva.

V Ljubljani, dne 23. septembra 2014 Podpis avtorja:

Za vso pomoč in nasvete pri izdelavi diplomske naloge se zahvaljujem mentorju, dr. Andreju Brodniku. Zahvale gredo tudi vsem zaposlenim na Arnesu, ki so mi omogočili izdelavo diplomskega dela. Zahvalila bi se tudi družini in prijateljem, ki so me tekom študija spodbujali in mi stali ob strani. Hvala vsem.

Mojim staršem.

Kazalo

Slike

Tabele

Listings

Seznam uporabljenih kratic

CA (*angl. Certification Authority*) Overitelj strežniških certifikatov.

CSR (*angl. Certificate Request*) Zahtevek za potrdilo.

DKIM (*angl. DomainKeys Identified Mail*) Elektronska pošta identificirana z domenskimi ključi.

DMARC (*angl. Domain-based Message Authentication, Reporting and Conformance*) Avtentikacija sporočil, poročanje in skladnost, ki temeljijo na domeni.

DNS (*angl. Domain Name Server*) Strežnik domenskih imen.

FQDN (*angl. Fully Qualified Domain Name*) Polno kvalificirano domensko ime.

IETF (*angl. Internet Engineering Task Force*) Delovna skupina za internetno tehniko.

IMAP (*angl. Internet Message Access Protocol*) Internetni sporočilni dostopni protokol.

IP (*angl. Internet protocol*) Internetni protokol.

ISP (*angl. Internet service provider*) Ponudnik internetnih storitev.

MDA (*angl. Mail Delivery Agent*) Agent za dostavo elektronske pošte.

MSA (*angl. Mail Submission Agent*) Agent za oddajo elektronske pošte.

MTA (*angl. Mail Transfer Agent*) Agent za prenos elektronske pošte.

MUA (*angl. Mail User Agent*) Uporabniški poštni agent.

PKI (*angl. Public Key Infrastructure*) Infrastruktura javnih ključev.

POP3 (*angl. Post Office Protocol version 3*) Poštni protokol verzije 3.

RFC (*angl. Request for Comments*) Zahtevek za komentar.

SASL (*angl. Simple Authentication and Security Level*) Preprosta avtentikacija in varnostna stopnja.

SMTP (*angl. Simple Mail Transfer Protocol*) Protokol za prenos elektronske pošte.

SPF (*angl. Sender Policy Framework*) Ogrodje pravil pošiljatelja.

SSL (angl. Secure Sockets Layer) Varna plast vtičnic.

TLS (angl. Transport Layer Security) Varnost transportne plasti.

URI (*angl. Uniform resource identifier*) Enolični identifikator vira.

Povzetek

V diplomskem delu spoznamo delovanje sistema elektronske pošte, kakšna je pri tem vloga DNS in ranljivosti protokola SMTP. Za nemoteno delovanje storitve je zelo pomembna ustrezna zaščita poštnega strežnika, kjer osnovno vlogo igrajo strežniški certifikati in varna povezava SSL. Dodatni varnostni mehanizem dosežemo z avtentikacijo e-pošte. V ta namen smo predstavili orodja SPF, DKIM in DMARC. SPF preverja naslov IP pošiljatelja in določa ali je le-ta avtoriziran za pošiljanje elektronskega sporočila z identificirano identiteto. DKIM poslanemu sporočilu doda domenski digitalni podpis in zavaruje vsebino sporočila. Z mehanizmom DMARC pa se na podlagi rezultatov obeh prejšnjih določi pravila, ki ciljnemu strežniku narekujejo, kakšen ukrep naj izvede nad prejetim sporočilom. Izvedli smo implementacije vseh omenjenih mehanizmov in ugotavljali o njihovi učinkovitosti delovanja.

Ključne besede: elektronska pošta, avtentikacija, poštni strežnik, SMTP, SPF, DKIM, DMARC.

Abstract

In this thesis, we learn in more detail about the functioning of the e-mail system, the role of the DNS, and the vulnerability of the SMTP. In order for the service to run smoothly, a suitable protection of the mail server is significant. Server certificates and SSL play a central role here. An additional way is achieved by e-mail authentication. To this purpose, we presented a variety of authentication mechanisms, SPF, DKIM, and DMARC. SPF checks the IP address of the sender and determines whether he or she is authorized to send e-mails with that identity. DKIM adds a digital signature to the sent e-mail and secures the content of the message. DMARC mechanism is based on the results of the two aforementioned authentication mechanisms. It specifies the rules for the destination server of the received message, dictating what action it should perform on it. We carried out the implementation of these mechanisms and tested their performance.

Keywords: e-mail, authentication, mail server, SMTP, SPF, DKIM, DMARC.

Poglavje 1

Uvod

Uporabniki storitev elektronske pošte se vsakodnevno soočajo z neželeno elektronsko pošto. Po poročanju varnostnih inženirjev Symantec Corporation [2], se je leta 2013, dnevno poslalo približno 29 bilijonov takšnih sporočil. To predstavlja 66,7 odstotkov vsega prometa elektronske pošte.

Naš cilj je postaviti poštni strežnik ter implementirati in preizkusiti napredne avtentikacijske mehanizme. Ti mehanizmi nam omogočajo zaščito domenskega imena, v imenu katerega se pošilja elektronska pošta iz našega strežnika. S tem želimo zagotavljati nemoteno in zanesljivo delovanje uporabnikom naše storitve. Z uporabo teh mehanizmov se zmanjša količina neželene elektronske pošte, ki bi se sicer lahko razpošiljala v našem imenu, saj so lahko takšna elektronska sporočila zavrnjena še preden pridejo v poštni predal uporabnika. Obenem sta zaščitena domena in poštni stražnik manj zanimiva za napadalce. Ob tem nam prav pride poznavanje ključnih pomanjkljivosti, ki jih predstavlja poštni sistem, da lahko uporabimo ustrezne metode za avtentikacijo elektronskih sporočil.

Diplomska naloga na začetku predstavi delovanje elektronske pošte ter elemente in poštne protokole, ki so potrebni za uspešno pošiljanje in prejemanje elektronskih sporočil. Nato spoznamo bistvene ranljivosti protokola SMTP, ki so pobuda za razpošiljanje neželene elektronske pošte in ugotavljamo s katerimi ukrepi jo lahko omejimo. V Poglavju 3 srečamo tudi s pojmom neželene elektronske pošte. Ker pri ukrepih proti neželeni pošti pomembno vlogo igra sistem DNS, v naslednjem poglavju podrobneje spoznamo tudi njegovo delovanje. Poglavje 4 nam predstavi napredne avtentikacijske mehanizme. Pouči nas o njihovem pomenu

implementacije za zaščito pred neželeno elektronsko pošto. Posamezne opisane mehanizme med sabo primerjamo in se srečamo s pomanjkljivostmi, ki jih prinaša posamezni mehanizem. Sledi praktični del diplomske naloge, kjer je predstavljena konfiguracija poštnega strežnika z ustrezno dodano zaščito strežnika ter implementacijo predhodno opisanih mehanizmov avtentikacije. Na koncu so podani še rezultati testiranja teh mehanizmov.

Poglavje 2

Elektronska pošta

Elektronska pošta je storitev, ki je že od vsega začetka prisotna med uporabniki interneta ter predstavlja pomembnejši del internetnih komunikacij. Namenjena je izmenjavi sporočil med posamezniki ali skupinami ljudi preko računalniških omrežij po celem svetu. Prvo elektronsko sporočilo je poslal Ray Tomlinson leta 1971, do leta 1996 pa je bilo poslano že več elektronskih sporočil, kot po navadni pošti. Danes elektronska pošta predstavlja predvsem hiter, poceni in preprost način komunikacije.

Elektronska sporočila se prenašajo med uporabniki, naslovljenimi z enoličnimi elektronskimi naslovi. Ti so oblike `<lokalni_del>@<domenski_del>`, pri čemer je znak »`@`« uporabljen kot ločevalnik v elektronskih naslovih in je obvezen za vse elektronske naslove SMTP. Lokalni del ponazarja uporabniško ime oz. naziv uporabnika, domenski del pa ime strežnika, kjer ima uporabnik poštni predal.

2.1 Struktura elektronskega sporočila

Format internetnega elektronskega sporočila definira standard RFC 5322 [3]. Elektronsko sporočilo sestavljata dve glavni komponenti, glava sporočila in telo sporočila.

V glavi sporočila (angl. *header*) vidimo različna polja, ki so sestavljena iz imen in pripadajočih vrednosti. Osnovna polja glave doda poštni odjemalec ob pošiljanju sporočila, dodatna polja pa so pripeta pri vsakem poštnem agentu, ki sporočilo prejme. Polja, ki jih doda posamezni poštni agent, sestavljajo ovojnico sporočila. Namenjena je napravam, ki skrbijo za prenos sporočila po internetu in ni vidna uporabnikom. Ovojnico sporočila definira standard RFC 5321 [4].

V nadaljevanju so prikazana nekatera imena polj glave sporočila z opisi posameznih vrednosti, ki so najbolj običajna:

`From:` Elektronski naslov pošiljatelja.

`To:` Elektronski naslovi enega ali več prejemnikov.

`Date:` Lokalni čas in datum napisanega sporočila.

`Subject:` Zadeva sporočila.

`Message-ID:` Enolični ID sporočila. Prepreči večkratno dostavo istega sporočila.

`In-Reply-To:` Vsebuje informacije zgornjega enoličnega ID sporočila, za katerega je poslan morebitni odgovor. S tem skupaj poveže sorodna sporočila.

`Cc:` Elektronski naslovi prejemnikov. V poštnih predalih so označeni ločeno od prejemnikov, podanih v polju `To:`.

`Bcc:` Elektronski naslovi prejemnikov. Ostalim prejemnikom so nevidni.

`Reply-To:` Elektronski naslov, kamor bo poslan morebitni odgovor na sporočilo.

`Received:` Zapis sledi, ki jo doda posamezni strežnik SMTP po prejemu sporočila.

`Return-Path:` Končni strežnik doda to polje na vrh glave sporočila. Vsebina je ustvarjena s SMTP ukazom `Mail from:`.

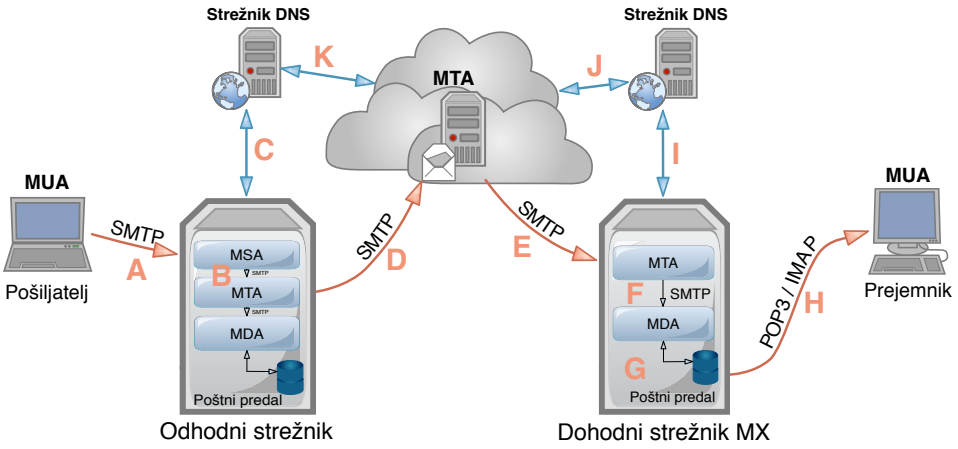
`Authentication-Results:` Rezultati preverjanja avtentikacije sporočila. [5].

RFC 5322 [3] sicer dovoljuje uporabo poljubnih polj, ki morajo obvezno biti v definirani obliki standarda: `izbirno-polje = ime-polja` ≫:≪ `nedoločeno-besedilo CRLF`. Pri tem je ime polja lahko sestavljeno iz izpisljivih znakov US-ASCII, z izjemo dvopičja ter presledka. Sledi mu znak za dvopičje, zatem pa še katero koli besedilo, ki ga lahko sestavljajo znaki US ASCII ter presledki, brez dodatnih omejitev. CRLF tu ponazarja novo vrstico. Izbirno polje ne sme biti povsem enako drugim poljem, definiranim v RFC 5322 [3].

Druga komponenta je telo sporočila (angl. *body*) in je od glave sporočila ločeno s prazno vrstico. Sestavlja ga besedilo, običajno šifrirano v ASCII kodi, ter morebitne priloge. Priloge podpira protokol MIME (angl. *Multi-Purpose Internet Mail Extensions*), ki je razširitev originalnega internetnega protokola in omogoča izmenjavo podatkovnih datotek, kot so npr. slikovne ali zvočne datoteke. [6]

2.2 Arhitektura in delovanje sistema elektronske pošte

Pri začetku procesa pošiljanja sporočila (Slika 2.1) se poštni odjemalec (MUA) poveže s poštnim strežnikom (MSA) z uporabo protokola SMTP (A). MSA nato sporočilo preda agentu za prenos elektronske pošte (MTA) (B), ki poskusi pridobiti podatke o ciljnem strežniku prejemnika na podlagi domenskega dela njegovega elektronskega naslova. To stori s pomočjo sistema DNS, ki skrbi za preslikovanje domenskih imen v naslove IP (C). Podrobnejše delovanje te storitve spoznamo v Poglavju 3. Ko MTA preko protokola DNS prejme ustrezni naslov IP ciljnega strežnika, se nato do njega poveže kot odjemalec SMTP z vzpostavitvijo seje SMTP (D,E). Če strežnik, ki prejme sporočilo, prepozna svojega uporabnika, ga preda poštnemu agentu za dostavo (MDA) (F). MDA dostavi sporočilo direktno v poštni predal prejemnika (G), ki lahko s poštnim odjemalcem preko protokola IMAP ali POP3 prebere sporočilo (H). Med prenosom lahko sporočilo potuje preko več strežnikov SMTP. Če se iz kakršnega koli razloga prvotni strežnik SMTP ne more povezati s strežnikom SMTP prejemnika, se sporočilo postavi v čakalno vrsto, kjer se skuša poslati periodično vsakih nekaj minut. V primeru neuspešne dostave se pošiljatelju po določenem času običajno vrne napaka oz. obvestilo o nedostavljivosti [7].



Slika 2.1: Prenos elektronske pošte od pošiljatelja k prejemniku.

2.3 Osnovni varnostni mehanizmi

Poštni promet med odjemalci in strežniki se prenaša v golem besedilu (angl. *plain text*). To besedilo lahko vsebuje informacije o uporabniških imenih, geslih, vsebini sporočil in ostalih občutljivih podatkih. V primeru, da se v komunikacijo med odjemalca in strežnik vrine napadalec, lahko ta s poslušanjem prometa razbere preneseno besedilo. Ker prvotni protokol SMTP [4] za pošiljanje sporočil ni ponujal uporabe gesla, je bila v ta namen razvita avtentikacija SMTP (angl. *SMTP authentication - SMTP AUTH*), pri kateri se odjemalec SMTP prijavi z uporabo avtentikacijskega mehanizma. Avtentikacija SMTP je razširitev SMTP protokola [8] in je definirana s standardom RFC 4954 [9].

Pri avtentikaciji SMTP se običajno uporabi avtentikacijski mehanizem z golim besedilom, ker je najpreprostejši in ga podpirajo vsi odjemalci. Za priključitev tega mehanizma v obstoječe aplikacijske protokole (SMTP, POP3, IMAP), se uporablja avtentikacija SASL (angl. *Simple Authentication and Security Layer*), definirana z RFC 4616. [10] SASL zavaruje dejansko avtentikacijo tako, da šifrira uporabniško ime in geslo uporabnika, medtem ko je ostalo sporočilo še vedno v golem besedilu. Zato avtentikacija SMTP zahteva uporabo varne povezave SSL (angl. *Secure Sockets Layer*), ki jo definira standard RFC 6101 [11].

SSL je standardna varnostna tehnologija za šifriranje povezave med odjemalcem in strežnikom. Ko je povezava SSL vzpostavljena, šifrira podatke za prenos med njima, prejeti podatki pa so nato dešifrirani ter dostavljeni do odjemalca oz. strežnika na aplikacijski plasti. SSL s tem poskrbi, da vsi podatki med odjemalcem in strežnikom ostanejo tajni ter jih lahko vidijo le za to namenjeni uporabniki.

Šifrirano povezavo SSL lahko dosežemo s kriptografijo javnega ključa. Ta vključuje dva ključa, zasebni in javni ključ, ki sta matematično povezana tako, da je operacija šifriranja izvedena z enim in se lahko z drugim dešifrira. Zasebni ključ je shranjen na določeni napravi, javni ključ pa je lahko javno objavljen oz. izmenjan pri sami komunikaciji. Tu se pojavi problem identifikacije lastnika javnega ključa, saj ga lahko objavi kdorkoli in tako npr. dobiva elektronsko pošto, ki je namenjena nekomu drugemu. Da javni ključ res pripada določeni identiteti, zagotovimo z digitalnim potrdilom in overjanjem.

Digitalno potrdilo javnega ključa je digitalni dokument, ki potrjuje povezavo med javnim ključem in določeno osebo ali organizacijo oz. strežnikom. To digitalno potrdilo je ponavadi v formatu standarda x.509 certifikata, ki ga definira RFC 5280 [12], njegovo dostopnost in procesiranje pa RFC 4210 [13]. Poleg podatkov o ključu, vsebuje tudi čas nastanka, informacije o lastniku, rok veljavnosti, ipd. Generiran certifikat s strani strežnika nato podpiše javen, zaupanja vreden overitelj digitalnih potrdil CA (angl. *Certificate Authority*). CA upravlja z digitalnimi certifikati ter predstavlja osrednjo vlogo v infrastrukturi javnih ključev (angl. *Public Key Infrastructure*). Preveriti mora informacije o osebi, ki certifikat naroča in zanesljivo ugotoviti njeno identiteto, zatem pa njen javni ključ podpiše s svojim zasebnim ključem. Overitelj mora ohranjati podrobne zapise o vseh izdanih certifikatih ter informacijah, uporabljenih za njihovo izdajo.

Isti digitalni certifikat lahko uporabimo tako za medsebojno identifikacijo strežnikov SMTP, kot tudi za šifrirano povezavo SSL med uporabnikom in strežnikom. Uporaba varne povezave SSL nam zagotavlja varnostne in avtentikacijske storitve, avtentikacijo strežnika, celovitost sporočila in avtentikacijo odjemalca za povezavo TCP skozi aplikacijsko plast.

2.4 Poštni agenti

Poštni agent je običajno programska oprema, ki skrbi za prenos elektronske pošte na uporabniški računalnik s poštnega strežnika. Poskrbi tudi za prikaz teh sporočil in druge bolj napredne funkcionalnosti, kot so hramba elektronskih naslovov oseb, s katerimi komuniciramo, razvrščanje in urejanje sporočil, ipd. Glede na njihov namen ločimo več tipov poštnih agentov. To so MUA, MTA, MSA in MDA.

2.4.1 Uporabniški poštni agent

MUA (angl. *Mail User Agent*) je uporabniški program, ki je v osnovi namenjen branju in pošiljanju elektronskih sporočil. Lahko se ga uporablja preko ukazne vrstice ali v grafični podobi, kot sta npr. znana programa *Mozilla Thunderbird* ali *Microsoft Outlook*. Kadar gre za program, nameščen na uporabnikovem sistemu, mu rečemo poštni odjemalec [14]. Da bi poštni odjemalci lahko prejemali in pošiljali sporočila, potrebujejo poštni strežnik, na katerega se lahko povežejo. Poštni sistem v osnovi sestavljata dva dela. En del skrbi za pošiljanje sporočil, drugi pa za prejemanje in dostavo v poštni predal. Del, ki skrbi za odhodna sporočila, se imenuje SMTP strežnik. Drugi del, ki služi prejemanju sporočil, pa je IMAP ali POP3 strežnik. Vsak izmed njih posluša in odgovarja na zahtevke, na za to namenjenih vratih TCP. To nam omogoča tudi to, da lahko oba strežniška sistema namestimo na en sam strežnik, ki opravlja obe vlogi.

2.4.2 Agent za prenos elektronske pošte

MTA (angl. *Mail Transfer Agent*) je programska oprema, odgovorna za prejemanje ali zavračanje dohodne pošte in pošiljanje odhodne pošte. Sporočilo lahko prejme preko TCP vrat 25 od drugega MTA ali pa od MSA oz. MUA s pomočjo protokola SMTP. Med tovrstne agente spadajo *Sendmail, Postfix, Microsoft Exchange, Courier*, ipd. [15]

2.4.3 Potrditveni poštni agent

MSA (angl. *Mail Submission Agent*) je komponenta MTA, ki sprejema elektronska sporočila od MUA z uporabo protokola SMTP. Uradna številka TCP vrat je 587, čeprav veliko ponudnikov elektronske pošte še vedno dovoljuje povezavo preko standardnih TCP vrat 25. Potrditvena elektronska pošta je definirana po standardu RFC 6409 [16]. Agenta MTA in MSA sta pogosto le različna primera iste programske opreme z različnimi možnostmi na isti napravi [17]. Njuna glavna razlika je, da je za MSA obvezna SMTP avtentikacija.

2.4.4 Agent za dostavo elektronske pošte

MDA (angl. *Mail Delivery Agent*) predstavlja poštni strežnik, ki skrbi za dostavo in shranjevanje sporočil od poštnega gostitelja v poštni predal uporabnika. Vsa prejeta sporočila privzeto shrani v format ≫`mbox`≪, kjer so združena in shranjena v eni datoteki. Novejši način shranjevanja sporočil, format ≫`maildir`≪, pa sporočila hrani v ločenih datotekah z enoličnimi imeni. Ko je sporočilo shranjeno na strežniku, ga je moč prebrati lokalno z uporabo MUA, ali preko protokolov POP3 oz. IMAP, katera uporabnikom omogočata oddaljeni dostop do poštnih predalov. MDA je zaščiten z uporabniškim imenom in geslom, da se prepreči branje sporočil drugih uporabnikov znotraj istega poštnega strežnika. Ker oba protokola prenašata informacije uporabnika v golem besedilu, je priporočena uporaba varne povezave SSL. Primera takega agenta sta *Dovecot* in *Procmail* [15].

2.5 Protokoli

2.5.1 Protokol POP3

Protokol POP3 (angl. *Post Office Protocol version 3*) se uporablja za prenos sporočil iz poštnega strežnika do poštnega odjemalca uporabnika. Definira ga standard RFC 1939 [18]. Ko MDA prejeto sporočilo dostavi v poštni predal ustreznega uporabnika, to pri formatu shranjevanja sporočil ≫`mbox`≪ stori tako, da vsebino sporočila pripne na konec datoteke. V primeru uporabe formata ≫`maildir`≪ pa ustvari edinstveno datoteko ter vanjo zapiše sporočilo.

Uporabnik lahko do vsebine poštnega predala dostopa s poštnim odjemalcem preko TCP vrat 110 oz. vrat 995, kadar je vzpostavljena varna povezava SSL. Po uspešni avtentikaciji, ki jo zahteva strežnik SMTP, se sporočilo prenese k uporabniku. Pri tem protokolu se nato vsebina poštnega predala privzeto izbriše.

2.5.2 Protokol IMAP

S prihodom novejših naprav in bolj zahtevnih uporabnikov, ki uporabljajo več kot eno napravo za dostop do svojega poštnega predala, je bil razvit protokol IMAP (angl. *Internet Message Access Protocol*). Definiran je z RFC 3501 [19] in v primerjavi s protokolom POP3 ponuja nekaj prednosti. Vsak povezan odjemalec komunicira s poštnim strežnikom in osvežuje stanje poštnega predala med vsemi napravami.

Vse akcije se zabeležijo neposredno na strežniku IMAP in hkrati na naši napravi. Poštni odjemalec se s strežnikom IMAP poveže z uporabo TCP vrat 143 in uporabniku dovoljuje usklajevanje statusov sporočil (prebrana, izbrisana, premaknjena) tudi med več poštnimi odjemalci [14]. Da lahko uporabnik dostopa do svojih sporočil tudi kadar nima vzpostavljene povezave z internetom, se kopija sporočil vseeno prenese na lokalni računalnik, ob naslednji povezavi pa se lahko prenesejo še vsa ostala morebitna nova sporočila. Za povezovanje preko varne povezave SSL, so protokolu IMAP dodeljena TCP vrata 993.

2.5.3 Protokol MAPI

Protokol MAPI (angl. *Messaging Application Programming Interface*) deluje na enak način, kot protokol IMAP, le da ima še nekaj dodatnih funkcionalnosti. Razvilo ga je podjetje Microsoft za svoje poštne odjemalce, kot je npr. *Microsoft Outlook*. Ti odjemalci se lahko sporazumevajo s poštnim strežnikom *Microsoft Exchange* preko komunikacije RPC (angl. *Remote Procedure Call*), definirane z RFC 5531 [20].

Dodatne možnosti tega protokola uporabniku omogočajo sinhronizacijo in pregled nad vsemi njegovimi mapami, pod-mapami, koledarjem ter shranjenimi podatki z različnih napravah, ki imajo nameščen MAPI. Vse te informacije so namesto na lokalnem računalniku uporabnika, shranjene na njegovem poštnem strežniku.

Protokol MAPI dovoljuje tudi vpogled v osnovne informacije, kot so zadeva sporočila ter ime in velikost priponke, še pred samim prenosom elektronskega sporočila. [21]

2.5.4 Protokol SMTP

SMTP (angl. *Simple Mail Transport Protocol*) je internetni protokol za prenos elektronske pošte med različnimi sistemi. Prvič je bil definiran leta 1982 z internetnim standardom RFC 821 in nazadnje posodobljen leta 2008 z razširitvenim SMTP (angl. *ESMTP - Extended Simple Mail Transport Protocol*). Ta je v uporabi danes in ga definira internetni standard RFC 5321 [4], ki določa pošiljanje elektronskih sporočil ter vzpostavitev in prekinitev komunikacijske seje. Za prenos podatkov uporablja protokol TCP/IP s pomočjo katerega privzeto preko TCP vrat 25 komunicira na aplikacijski plasti. Povezave SMTP z varno povezavo SSL uporabljajo privzeta TCP vrata 465, pri potrditveni elektronski pošti (angl. *mail submission*) pa protokol posluša na TCP vratih 587 [22].

Medtem ko poštni strežniki in ostali MTA uporabljajo SMTP za pošiljanje in prejemanje poštnih sporočil, odjemalec na uporabnikovem sistemu običajno uporablja SMTP le za pošiljanje sporočil do MTA, za prejemanje pa protokol POP3 ali IMAP [22]. Komunikacija med strežniki SMTP poteka po principu odjemalec-strežnik. Kadar želi odjemalec SMTP posredovati sporočilo, vzpostavi dvosmerni prenosni kanal do strežnika SMTP, običajno preko protokola TCP/IP. Sporočilo nato posreduje naprej do enega ali več strežnikov SMTP in ustrezno poroča o uspešnosti prenosa podatkov. Prenos sporočil se lahko zgodi z eno samo povezavo med originalnim pošiljateljem SMTP in končnim ciljem SMTP, ali pa v nizu skokov skozi vmesne sisteme, kjer posamezni vmesni strežnik SMTP prevzame vlogo odjemalca SMTP.

Vsak MTA prejetemu sporočilu v glavo doda polje `Received:`, kamor pripne podatke o identiteti strežnika, času prejema sporočila, ter kateremu strežniku je bilo sporočilo posredovano naprej.

Tipi sistemov SMTP

Ločimo štiri tipe sistemov SMTP na osnovi vlog, ki jih igrajo pri prenosu elektronske pošte:

1. **Izvor (angl. *originating*)** Ta sistem sporočilo predstavi okolju prenosne storitve.

2. **Dostava (angl. *delivery*)** Prejme sporočilo od okolja prenosne storitve, ga preda MUA ali dostavi v shrambo sporočil, do koder dostopa MUA.

3. **Posredovanje (angl. *relay*)** Prejme sporočilo od odjemalca SMTP in ga posreduje do drugega strežnika SMTP. Ponavadi predstavlja cilj zapisa MX poizvedbe DNS. Strežnik lahko sprejme ali zavrne zahtevek za posredovanje sporočila. V primeru zavrnitve vrne odgovor 550, drugače pa sam postane odjemalec SMTP in vzpostavi povezavo do naslednjega strežnika SMTP, zavedenega v DNS in mu posreduje sporočilo. Če strežnik SMTP kasneje ugotovi, da sporočilo iz kakršnega koli razloga ne more biti dostavljeno, pošlje obvestilo o neuspešni dostavi do izvornega pošiljatelja.

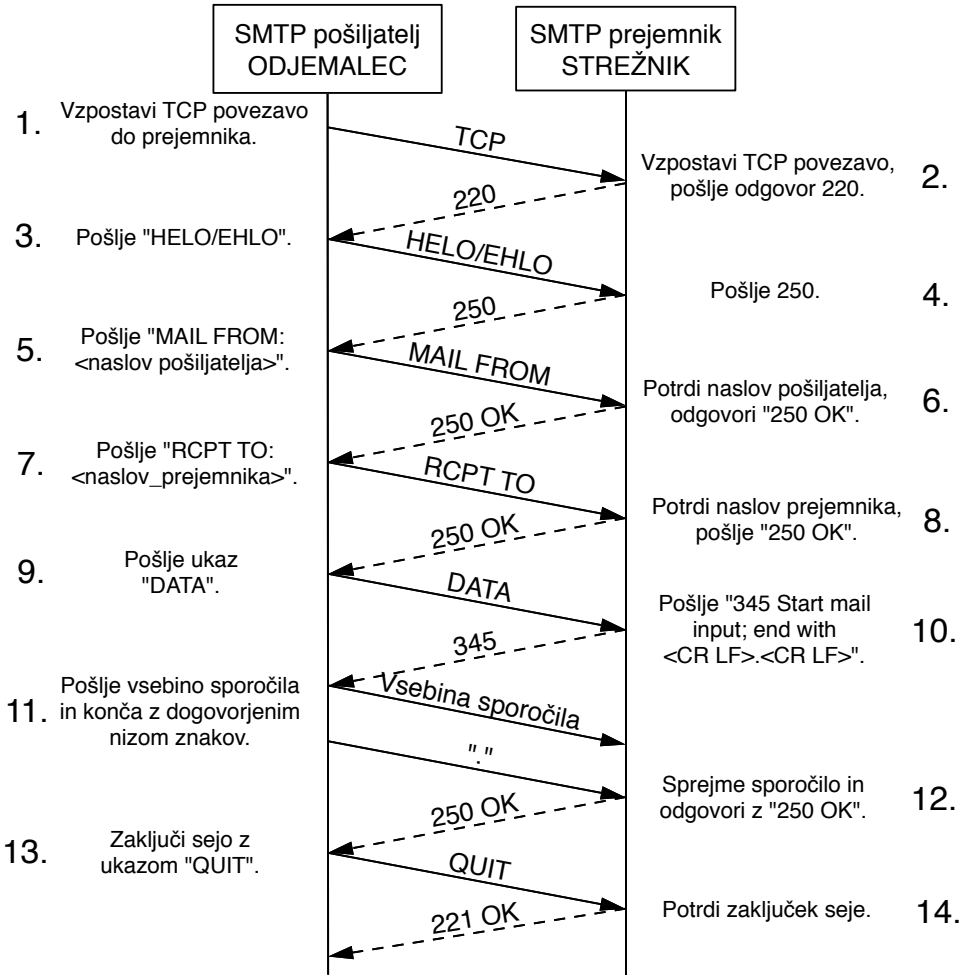
4. **Prehod (angl. *gateway*)** Prejme sporočilo od sistema odjemalca enega prenosnega okolja in ga posreduje do sistema strežnika drugega prenosnega okolja. Med enim in drugim sistemom mora ponavadi zaradi različnih protokolov in formatov sporočil, strežnik SMTP izvesti prevajalne algoritme [4].

Odgovori SMTP

Odgovori SMTP so namenjeni temu, da odjemalec SMTP vedno pozna stanje strežnika SMTP. Sestavljeni so v spodnji obliki, pri čemer `<SP>` pomeni presledek, `<CRLF>` pa ponazarja novo vrstico:
`trištevilčna koda, <SP>, vrstica besedila, <CRLF>`
Trištevilčna koda ima poseben pomen. Prva številka kode nam pove, ali je odgovor pozitiven (`2xx`) ali negativen začasno (`4xx`) oz. trajno (`5xx`). Iz druge številke odjemalec SMTP lahko razbere vrsto napake, zadnja pa predstavlja najvišjo stopnjo informacije.

Ukazi in seja SMTP

Seja SMTP se začne, ko odjemalec vzpostavi TCP povezavo do strežnika (1), ta pa mu odgovori z odpiranjem sporočila (2). Odjemalec nato strežniku pošlje ukaz `EHLO` s katerim označuje svojo identiteto oz. ukaz `HELO` v primeru, da ne podpira zahtev razširitvenega načina v sproženi seji (3). Strežnik mu odgovori z `250 OK` (4). V nadaljevanju SMTP prenos sestoji iz treh zaporedij ukazov.



Slika 2.2: Seja SMTP med odjemalcem in strežnikom.

Odjemalec z ukazom `MAIL FROM:` strežniku SMTP nakaže nov prenos sporočila in hkrati poda informacijo o izvornem poštnem predalu, kamor se pošlje morebitno obvestilo o napaki (5). MTA običajno preveri, če je vneseni naslov veljaven. V primeru da ni napak, je odgovor strežnika `250 OK` (6). S strani odjemalca nato lahko sledi eden ali več `RCPT TO:` ukazov zapored (7). Njegov podani argument določa prejemnika, na kar strežnik vrne odgovor `250 OK` oz. napako, če naslov ni veljaven (8). Ko odjemalec pošlje ukaz `DATA`, s tem naznani začetek besedila sporočila (9). Strežnik mu najprej pošlje odgovor `345`, s katerim pove, da je pripravljen sprejeti besedilo (10). Odjemalec pošlje vsebino sporočila in konec podatkov označi z vrstico, ki vsebuje le znak »`.`« (11). Ko je konec besedila uspešno prejet in shranjen, mu strežnik odgovori še z `250 OK` (12). Znotraj iste seje se lahko postopek zgornjih treh zaporedij ukazov ponovi. Za zaprtje seje se na koncu poda ukaz `QUIT` (13). V odgovor na ta ukaz mora prejemnik poslati 221 OK ter zapreti prenosni kanal (14).

Sejo SMTP lahko sestavlja še nekaj dodatnih ukazov. Ukaza `VRFY` in `EXPN` se uporabljata za preverjanje elektronskega naslova prejemnika oz. poštnega seznama in za pozitiven rezultat vrneta odgovor `250 OK`. Če se izvede `RSET`, pomeni, da bo trenutni prenos sporočila prekinjen. Vsi prejeti podatki morajo biti zavrženi. Če želimo, lahko z ukazom `HELP` od odjemalca prejmemo uporabne informacije o nekem ukazu [4]. Prikaz običajne komunikacije med odjemalcem in strežnikom nakazuje Slika 2.2.

2.6 Ranljivosti protokola SMTP

Protokol SMTP že v samem začetku ni bil zasnovan kot varen protokol. Elektronska pošta je bila takrat namenjena le ožjim uporabnikom in je delovala kot povsem zaupanja vreden vir komunikacije. Implementacija SMTP je bila zato naravnana predvsem k temu, da kakršno koli elektronsko pošto zanesljivo dostavi do prejemnika.

Ker protokol SMTP ne preverja avtentikacije izvora sporočila, pomeni, da lahko kdor koli pošlje sporočilo v imenu poljubne identitete. Definira prenos sporočila in ne njegove vsebine, kar pomeni, da določa le ovojnico sporočila, medtem ko ga njegova glava in telo sporočila ne zanimata. Obenem je nešifrirana vsebina sporočila

vidna vsaki osebi oz. napravi, ki uspe prestreči komunikacijo med pošiljateljem in prejemnikom sporočila.

Veliko težavo predstavljajo strežniki SMTP za posredovanje, ki jih lahko napadalec izkoristi za zlorabo podatkov in razpošiljanje neželene elektronske pošte. To pomanjkljivost izkoriščajo napadalci predvsem za gradnjo robotskih omrežij računalnikov (angl. *botnet*), preko katerih se razpošiljajo ogromne količine tovrstnih elektronskih sporočil. Zaradi tega večina administratorjev omeji dostop do poštnega strežnika od zunaj. Tako je posredovanje sporočil možno le znotraj lastnega omrežja ali med uporabniki, ki so avtenticirani s strežnikom. Seveda lahko napadalci še vedno postavijo svoj strežnik SMTP ter preko njega pošiljajo večje količine neželene elektronske pošte v relativno kratkem časovnem obdobju.

Danes je poštna infrastruktura tako ogromna, da je uvajanje sprememb v protokol SMTP praktično nemogoče. S tem bi najverjetneje povzročili nedelovanje večine poštnih strežnikov. Delno rešitev ponujajo določeni mehanizmi, ki jih dodamo poštnemu sistemu. Za zaščito pred neželeno pošto lahko poskrbimo pred ali po prejemu sporočila.

Pred prejemom elektronskega sporočila lahko preverimo lastnosti pošiljatelja in na podlagi rezultatov sprejmemo oz. zavrnemo njegovo sporočilo. V pomoč so nam črni (angl. *blacklists*) in beli seznami (angl. *whitelists*). Črni seznami vsebujejo elektronske in IP naslove, ki so znani po pošiljanju neželene elektronske pošte, beli pa vsebujejo zaupanja vredne pošiljatelje. Ker napadalci največkrat zlorabljajo tuje elektronske in IP naslove, se na črnem seznamu pogosto znajdejo nedolžne osebe in naprave.

Prejeto elektronsko pošto lahko preverjamo z analizo vsebine sporočila. Filtriramo lahko na podlagi ključnih besed v sporočilu in hevurističnih algoritmov. Tu je nujna izjemna previdnost, saj lahko legitimna sporočila ocenimo za neželena.

Obstaja več različnih mehanizmov, ki ponujajo avtentikacijo na nivoju prenosa in s tem izboljšujejo obstoječo situacijo. Med najbolj uporabljanimi so mehanizmi SPF [23], DKIM [24] in DMARC [25].

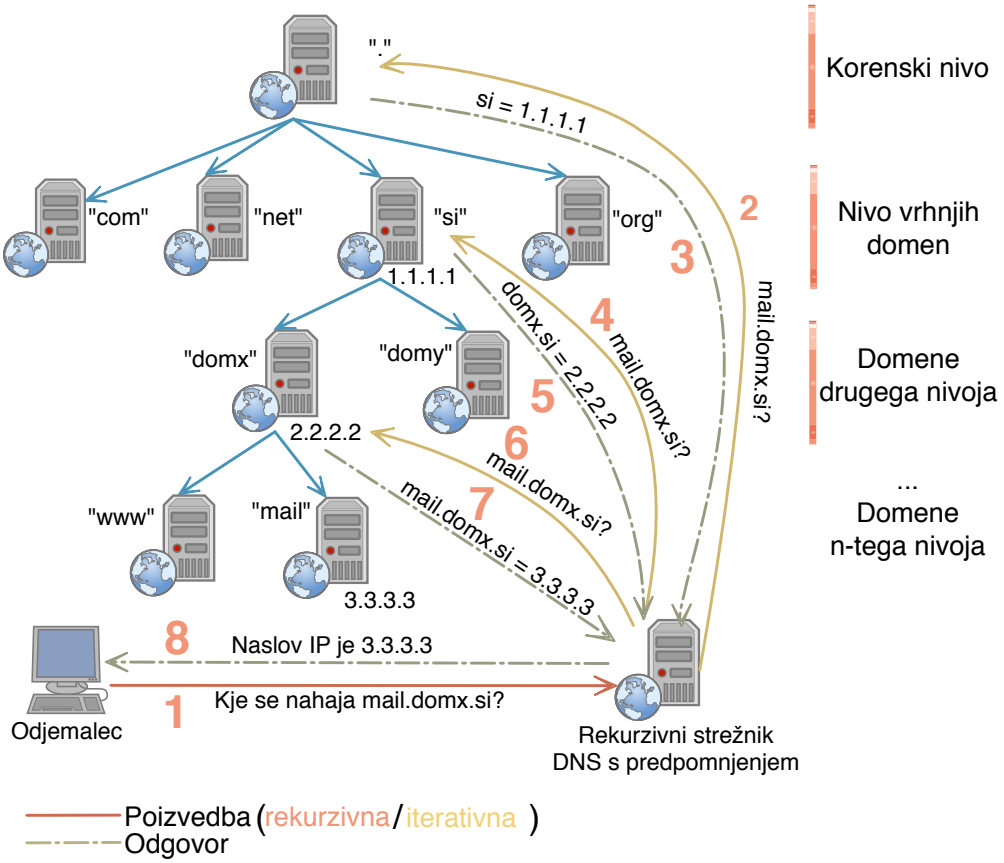
Poglavje 3

DNS

Vsaka naprava v internetnem omrežju je enolično določena z naslovom IP, ki poskrbi za identifikacijo med njimi. Za dostop do posamezne naprave se uporablja tudi polno internetno domensko ime ali FQDN (angl. *Fully Qualified Domain Name*), ki si ga je lažje zapomniti. Ker FQDN ni naslov s pomočjo katerega se lahko naprave med seboj naslovijo, se v ta namen uporabi sistem DNS. DNS (angl. *Domain Name Server*) vzdržuje bazo domenskih imen ter njim pripadajoče naslove IP in tako poskrbi za preslikavo med naslovom IP in FQDN. Definirata ga RFC 1034 [26] in RFC 1035 [27].

3.1 Porazdeljenost in hierarhija

DNS je distribuirana podatkovna baza, kar omogoča lokalen nadzor segmentov skupne baze podatkov, podatki vsakega segmenta pa so dosegljivi po celotnem omrežju preko sistema odjemalec-strežnik. Celotna podatkovna baza DNS je strukturirana kot drevo, pri čemer ima na vrhu drevesa korensko vozlišče, predstavljeno s $\gg . \ll$. Taka struktura zagotavlja enoličnost domenskih imen. Za lažjo predstavo nam je v pomoč Slika 3.1.



Slika 3.1: Postopek poizvedbe na strežnik DNS.

Vsako vozlišče v drevesu je koren novega poddrevesa, ki predstavlja del skupne podatkovne baze oz. domensko ime. Vse domene se lahko razdeli naprej na pod-domene. Posamezno domensko ime je enolično in nakazuje lokacijo v podatkovni bazi DNS. Polno domensko ime katerega koli vozišča v drevesu je zaporedje oznak na poti od tega vozlišča do korena drevesa. Imena so vedno prebrana v tem vrstnem redu, od vozlišča do korena, pri tem pa so posamezne oznake ločene s piko, kar predstavlja tudi posamezni nivo v domenski strukturi.

Eden izmed glavnih ciljev strukture DNS je bil razdelitev administracije, kar dosežemo z dodeljevanjem odgovornosti na posamezno organizacijo. Pri tem se lahko vsaka pod-domena dodeli drugi organizaciji in ta organizacija nato postane

odgovorna za upravljanje podatkov v tej pod-domeni. Organizacija lahko podatke spreminja in razdeli svojo pod-domeno naprej na pod-domene, katere lahko zopet dodeli drugim organizacijam. Gre pravzaprav za prenos odgovornosti nekega dela domene drugi organizaciji.

Vse vrhnje domene in večina domen drugega nivoja, so z dodeljevanjem razdeljene v manjše enote, lažje za upravljanje. Tem enotam rečemo cone (angl. *zone*). Sestavljajo jih vsa domenska imena, ki pripadajo posamezni domeni cone, z izjemo imen, ki spadajo v naprej dodeljene pod-domene. Informacije o coni shranjujejo imenski strežniki (angl. *nameservers*). Domena namreč lahko vključuje več informacij, kot jih potrebuje nek imenski strežnik, saj lahko vsebuje tudi informacije, dodeljene drugemu imenskemu strežniku. Pri ustvarjanju dodatnih con je najvišje ležeče vozlišče nove cone avtoritativno za svoja nižje ležeča vozlišča, stara cona pa je avtoritativen vir za novo cono. Če torej eden izmed domenskih strežnikov vpraša za podatke v neki pod-domeni, lahko prejme odgovor s seznamom avtoritativnih imenskih strežnikov, na katere se lahko obrne. [28]

Če imamo na primer domensko ime `www.en.snupi.si`, vidimo, da je njegova vrhnja domena `si`, za katerega odgovornost nosi določena organizacija. Domeno `primer` je dodelila drugi organizaciji. Vzemimo še, da je ta domena svoji pod-domeni `en` in `drugi`, zopet dodelila naprej posameznim organizacijam. V tem primeru bodo cono domene `snupi.si` sestavljale pod-domene `en`, `drugi` in bo za njiju predstavljala avtoritativen vir. Za vse morebitne pod-domene teh dveh pod-domen, pa bo avtoritativen vir predstavljala vsaka izmed njiju za vse svoje pod-domene. Tako v našem primeru pod-domena `www` sodi v cono domene `en` in je tudi njen avtoritativni vir.

3.1.1 Tipi imenskih strežnikov DNS in zapisi virov

Večji del mehanizma odjemalec-strežnik predstavljajo imenski strežniki, ki vsebujejo informacije o nekaterih segmentih podatkovne baze in preko katerih je ta informacija dostopna odjemalcem. Imenujejo se razreševalniki (angl. *resolvers*). Ti ustvarijo poizvedbo in jo pošljejo po omrežju do imenskega strežnika. Primer poizvedbe je prikazan na Sliki 3.1 (≫Kje se nahaja mail.domx.si?≪), opisana je v Poglavju 3.2. Tako poizvedbo lahko strežnik DNS prejme za katero koli domeno. Večina poizvedb pride za domene, za katere nima lokalnih podatkov. Zato obsta-

jata dve drsti poizvedb, iterativna in rekurzivna poizvedba. Prva poizvedba lahko vrne celoten odgovor ali napoti do drugega strežnika DNS, druga pa vedno vrne celoten odgovor. Razlikujemo več vrst imenskih strežnikov, opisanih spodaj.

Korenski strežniki

Predstavljajo osnovo DNS in so na vrhu drevesne hierarhije domen. Poznajo naslove IP vseh avtoritativnih strežnikov, ki upravljajo s poizvedbami DNS za vrhnje domene (angl. *top level domain*), kot je npr. ≫`.si`≪ domena. Na svetu je takih strežnikov 13.

Avtoritativni strežniki

So avtoritativni vir za vse informacije, ki jih rekurzivni strežniki vrnejo odjemalcem. Določeni so za vsako domeno. Ločimo dva tipa avtoritativnih strežnikov, ki skupaj skrbita za uravnoteženo obremenitev vseh zahtev. Prvi je primarni (gospodar), ki ima lokalno shranjene datoteke podatkovne baze. Drugi pa sekundarni (suženj), ki hranijo kopijo baze primarnega strežnika DNS in hkrati služi kot varnostna kopija teh podatkov.

Rekurzivni strežniki s predpomnjenjem

Za neko periodo časa (običajno 24 ur) si zapomnijo poizvedbe ter odgovore na njih, ki so jih prejeli s strani avtoritativnih strežnikov. S tem se prihrani na pasovni širini in času razreševanja domenskih imen. Za posamezni zapis administrator domene določi tudi časovno periodo (angl. *TTL - Time To Live*), da doseže ažurnost podatkov.

Zapisi virov DNS

Vsako vozlišče drevesa ima nič ali več zapisov virov (angl. *resource records*). Ti zapisi predstavljajo osnovni podatkovni element v sistemu DNS in vsebujejo informacije, povezane z določenim domenskim imenom. Korensko območje vsebuje le zapise virov za avtoritativne domenske strežnike posamezne domene. Zapisi virov so lahko različnih tipov, nekaj najpogostejših je opisanih v Tabeli 3.1.

Tip zapisa	Opis
`A`	Domensko ime preslika v 32-bitni naslov IPv6.
`AAAA`	Domensko ime preslika v 128-bitni naslov IPv6.
`CNAME`	Nastavi alias za domensko ime.
`MX`	Zapis, ki določa naslov poštnega strežnika. Delovanje poštnih sistemov se močno nanaša na to vrsto zapisov.
`PTR`	Pri obratnih poizvedbah preslika naslov IP v domensko ime.
`NS`	Za domeno določi ime avtoritativnega strežnika, ki dovoljuje DNS poizvedbe znotraj različnih con.
`SOA`	Določi strežnik DNS, ki upravlja z določeno domeno in njenimi informacijami.
`TXT`	Administrator lahko vstavi poljubno besedilo v zapis DNS.

Tabela 3.1: Tipi zapisa virov DNS.

3.2 Postopek poizvedbe na strežnik DNS

Vedno, kadar želimo dostopati do spletne strani ali poslati elektronsko sporočilo, se mora domensko ime preslikati v omrežni naslov. V primeru, da strežnik DNS ne najde podatka o preslikavi določenega domenskega imena, naredi poizvedbo do naslednjega strežnika DNS, dokler ne najde pravilnega naslova IP. Ko je omrežni naslov najden, strežnik posreduje svoj zahtevek na ta naslov. Primer poizvedbe DNS prikazuje Slika 3.1, postopek pa je sledeč: [29]

1. Odjemalec pošlje poizvedbo, podobno vprašanju: »Kje se nahaja mail.domx.si?«, do lokalno nastavljenega rekurzivnega strežnika DNS.

2. Rekurzivni strežnik preveri, če ima naslov `mail.domx.si` v svojem predpomnilniku. V primeru da ga ima, odgovor takoj vrne odjemalcu. Sicer poizvedbo za naslov `mail.domx.si` pošlje do korenskega strežnika.

3. Korenski strežnik ne pozna odgovora za poizvedbo domene `mail.domx.si`, ima pa podatke o naslednjem nivoju, v tem primeru `.si`. Rekurzivnemu

strežniku odgovori s podatkom o naslovu IP, kjer se nahaja strežnik za vrhovno domeno.

4. Rekurzivni strežnik pošlje enako poizvedbo tokrat do avtoritativnega strežnika za domeno `domx.si`, ki se v našem primeru nahaja na IP naslovu 1.1.1.1.

5. Vrhnji strežnik ima podatke o domeni `domx.si`, ne ve pa ničesar o `mail.domx.si`. Njegov odgovor vsebuje podatke o imenskem strežniku za `domx.si`.

6. Rekurzivni strežnik do strežnika na naslovu IP 2.2.2.2 zopet pošlje enako poizvedbo.

7. V podatkih cone `domx.si` vprašani strežnik najde podatke o zapisu A za domeno `mail.domx.si` in rekurzivnemu strežniku vrne polni odgovor.

8. Rekurzivni strežnik lahko sedaj odjemalcu vrne odgovor »Kje se nahaja mail.domx.si? = 3.3.3.3«, in nato to informacijo za določen čas shrani v svoj predpomnilnik.

9. Ko odjemalec prejme odgovor, lahko prične z vzpostavitvijo seje do strežnika na naslovu 3.3.3.3.

3.3 Vpliv DNS na elektronsko pošto

Sistem DNS ima velik pomen za infrastrukturo elektronske pošte. Ponuja mehanizme, ki za dostavo elektronske pošte določajo več poštnih strežnikov. Poštnim strežnikom omogoča tudi, da prevzamejo odgovornost za prenos sporočila od enega do drugega poštnega strežnika. Hkrati za posamezni ciljni strežnik dovoljuje poljubna domenska imena, en cilj pa lahko predstavlja tudi več poštnih strežnikov. Te funkcionalnosti dajejo administratorjem več fleksibilnosti za konfiguracijo elektronskih sporočil v njihovem omrežju.

Za usmerjanje elektronske pošte potrebuje sistem DNS en zapis vira. To je zapis MX, ki za neko domensko ime predstavlja poštni strežnik MX (angl. *mail exchanger*) (glej Sliko 2.1). Za domeno prejemnika odhodni strežnik preveri ciljni naslov strežnika MX s pomočjo sistema DNS. Po prejetem odgovoru od rekurzivnega strežnika DNS lahko elektronsko sporočilo dostavi v poštni predal prejemnika,

ga pošlje ciljnemu poštnemu strežniku oz. drugemu strežniku MX, ki bližje ciljnemu ali pa preda drugemu prenosnemu okolju.

Za posamezno domensko ime lahko obstaja več poštnih strežnikov MX, npr. `mail1.domena.si` in `mail2.domena.si`, za domensko ime `domena.si`. Zapis MX poleg domenskega imena strežnika zato vsebuje dodaten parameter, ki določa prioriteto posameznega strežnika, pri čemer najnižja vrednost pomeni najvišjo prioriteto. Z določanjem prioritete se prepreči zanka pri usmerjanju elektronske pošte. Poštni strežniki glede na prioriteto zapisa usmerijo elektronsko pošto do strežnika z najvišjo prioriteto, pri čemer najvišja prioriteta pomeni najnižjo vrednost. V primeru, da je ta strežnik nedosegljiv, pa se sporočilo pošlje do strežnika z naslednjo najvišjo prioriteto, če ta obstaja [28].
Primer zapisa: `snupi.si IN MX 10 mail1.snupi.si`

Sistem DNS je postal zelo uporaben tudi pri zaščiti elektronske pošte. Poštnim strežnikom pomaga ločevati med viri legitimnih in neželenih sporočil. Novi mehanizmi v DNS namreč omogočajo preverjanje, kdo lahko pošilja sporočila v imenu določene domene. Strežniki, ki so pozorni na ta zapis v DNS lahko zavrnejo sporočila, ki ne prihajajo iz dovoljene naprave. S temi mehanizmi se bomo spoznali v Poglavju 4.

3.4 Ranljivosti DNS

Ko je zaradi vsesplošne uporabe interneta postala avtentikacija in zaščita podatkov nujna, so bili tarča napadov tudi strežniki DNS. Za preprečevanje zlorab in napadov so bile ustanovljene razne skupnosti, ki skrbijo za celovitost in nemoteno delovanje sistema. Do napadov sistema DNS lahko pride zaradi pomanjkljivosti v implementaciji protokola DNS, kot tudi na nivoju strežnika. V večini primerov se jim lahko izognemo z rednim posodabljanjem strežnika in spremljanjem novo-odkritih hroščev oz. ranljivosti.

Ena izmed težav je namerna ali nenamerna okvara podatkov v datotekah con, ki se nahajajo na samem imenskem strežniku. Nevarnost lahko predstavlja tudi oddaljeni administrator, ki lahko izvede neavtorizirane posodobitve. To lahko doseže s ponarejanjem naslova IP (angl. *IP address spoofing*) in s tem zakrije pravi izvor pošiljatelja. Ponarejanje naslova IP se lahko izrabi tudi pri prenosu

podatkov med posameznimi conami s čimer napadalec doseže preusmeritev odjemalca na drug naslov IP. Uporabnik se pri tem ne zaveda, da ni preusmerjen na pravi strežnik [29].

Dostopnost strežnika se izrablja predvsem pri DOS napadu (angl. *denial-of-service*). Tega lahko povzroči zlonamerni napadalec oz. nenamerno uporabnik ali sistem. Pri tem napadu so storitve DNS preobremenjene z zahtevki in posledično postanejo nedosegljive. Izognemo se mu z omejevanjem števila poizvedb.

Pomanjkljivosti v samem protokolu DNS in njegovih različnih implementacijah, omogočajo zastrupljanje predpomnilnika (angl. *cache poisoning*). Z izrabo ranljivosti lahko napadalec podtakne lažne DNS podatke v predpomnilnik in tako preusmeri promet iz legitimnih strežnikov na lažne. Točko tega napada lahko v našem primeru predstavlja rekurzivni strežnik na Sliki 3.1. Najboljšo rešitev predstavlja DNSSEC, ki je varnostna razširitev protokola DNS ter omogoča avtentikacijo in celovitost DNS podatkov. Definirana je s standardi RFC 4033 [30], 4034 [31] in 4035 [32].

Poglavje 4

Avtentikacijske metode elektronskih sporočil

Protokol SMTP dovoljuje dostop do strežnika brez kakršnih koli prijavnih podatkov uporabnika. Posledično dovoljuje poneverjanje pošiljateljevega naslova. Posledica teh slabih lastnosti je, da omogoča ne-overjenim uporabnikom pošiljanje sporočil v imenu drugih. Danes se velika količina neželene elektronske pošte razpošlje ravno zaradi zlorabe te možnosti. Ponarejanje naslova predstavlja nevarnost za uporabnike in podjetja ter hkrati ogroža celotno elektronsko poštno infrastrukturo, saj zmanjšuje zaupanje ljudi v svojo zanesljivost. Žrtvam se zaradi takih zlorab zmanjša njihov ugled, zavračati pa morajo tudi odgovornost za zlorabe. Ker je uporaba poljubnega domenskega imena precej preprosta, so upravičeno zaskrbljeni tudi lastniki domen.

Kot smo spoznali do sedaj, pri preprečevanju neželene elektronske pošte bistveno vlogo igra ustrezna zaščita poštnega strežnika in dodatni mehanizmi, s pomočjo katerih lahko občutno zmanjšamo nadležno pošto. Mednje sodijo avtentikacijski mehanizmi, ki odhodna sporočila opremijo s preverljivimi informacijami in se ponavadi izvajajo na nivoju domenskih imen.

Avtentikacija elektronskih sporočil (angl. *email authentication*) je način, s katerim lahko ponudniki poštnih storitev preverijo identiteto dohodnih elektronskih sporočil in s tem zmanjšajo uspešno dostavo ne-legitimne elektronske pošte. Hkrati je izjemno pomembna za lastnike domenskih imen, v imenu katerih se elektron-

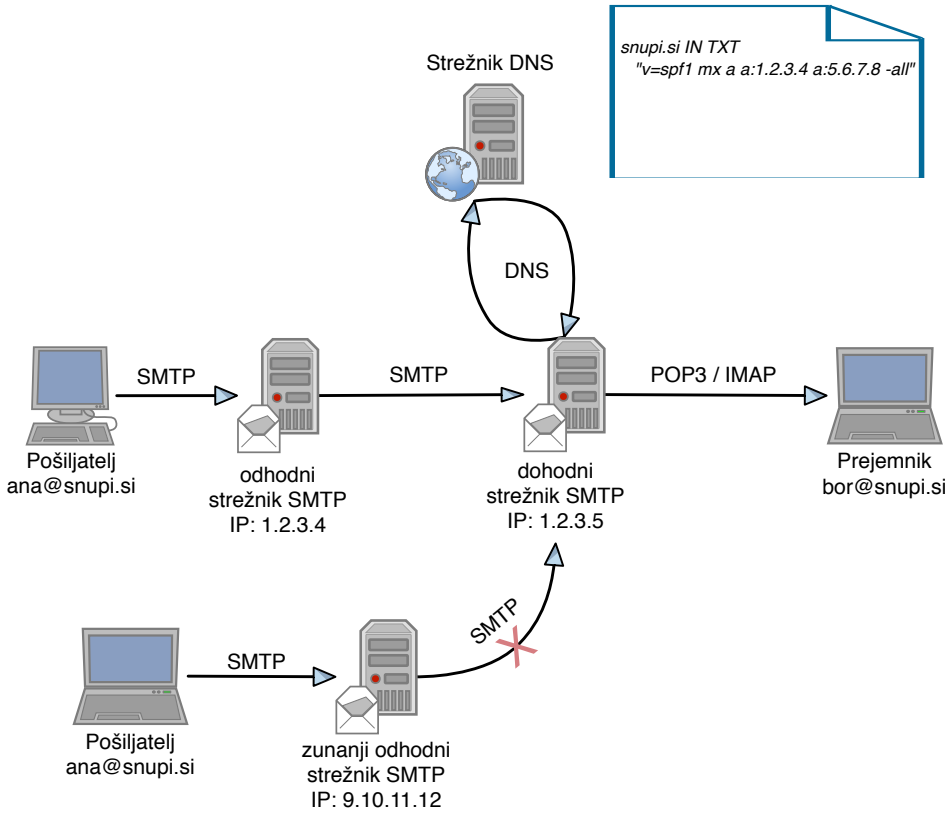
ska pošta pošilja. Z uporabo ustreznih avtentikacijskih mehanizmov se zavaruje ime in ugled pošiljateljeve domene ter prepreči njena lažna predstavljanja. V tem poglavju se bomo posvetili trem metodam, ki jih v večini uporabljajo vsi večji ponudniki elektronskih poštnih storitev.

4.1 Ogrodje pravil pošiljatelja

Ogrodje pravil pošiljatelja (SPF - angl. *Sender Policy Framework*) je dokaj preprosta avtentikacijska metoda. Njegova prva specifikacija je bila izdana v sredini leta 2003, naslednjim so sledile dodatne podrobnosti, trenutna končna specifikacija pa definirana v IETF publikaciji s standardom RFC 7208 [23].

Uporaba varnostnega mehanizma SPF omogoča lastnikom domen, da določijo avtorizirane strežnike SMTP za pošiljanje elektronske pošte v njihovi domeni, katere identiteta je vidna dohodnemu strežniku MTA v seji SMTP z ukazom `MAIL FROM` ali `HELO` (oba sta v sklopu SMTP specifikacije definirana v RCF 5321 [4]). Pri tem mu pomaga sistem DNS z enoličnim zapisom TXT za mehanizem SPF. Tu ima DNS nekoliko drugačno funkcijo kot za zapis MX. Medtem ko zapis MX pove pošiljajočemu MTA, kateremu poštnemu strežniku naj pošlje sporočilo, naslovljeno na določeno domensko ime, informacija zapisa SPF prejemajočemu MTA pove, katerim poštnim strežnikom je dovoljeno pošiljanje sporočil, naslovljenih z določenim domenskim imenom. Sporočila, ki prihajajo od neavtoriziranih virov, so lahko tako zavrnjena že pred samim prejemom telesa sporočila. Lokalna pravila strežnika SMTP nato ukrepajo na podlagi pošiljateljeve domene in ostalih poštnih elementov, brez nadaljnjega preverjanja naslova IP.

Poglejmo si primer delovanja mehanizma SPF pri pošiljanju sporočila iz elektronskega naslova `ana@snupi.si`, ki ga ponazarja Slika 4.1. Pri pošiljanju sporočila takoj po vzpostavitvi povezave dohodni strežnik sprejme SMTP ukaz `HELO` in `MAIL FROM`, ki je viden v glavi sporočila. Oba lahko vsebujeta domensko ime, v našem primeru je to `snupi.si`. Dohodni strežnik pošlje poizvedbo za zapis SPF, označen s tem domenskim imenom, do strežnika DNS. Nato v zapisu zavedene naslove IP, avtorizirane za uporabo domene `snupi.si`, primerja z naslovom IP odhodnega strežnika in vrne rezultat (glej 4.1.1). V kolikor domena avtorizira naslove IP, je sporočilo uspešno avtenticirano [33].



Slika 4.1: Delovanje avtentikacijskega mehanizma SPF.

Z dodajanjem zapisa za SPF v sistem DNS, se lažna predstavljanja domene zmanjšajo, saj je večja verjetnost, da se takšna elektronska pošta ujame v filtre neželene pošte, ki preverjajo ta zapis. Hkrati je zaščitena domena za napadalce manj uporabna pri razpošiljanju neželene elektronske pošte. Uporaba mehanizma SPF pokaže veliko prednost predvsem pri polju `Return-Path` v glavi sporočila. Tu je namreč zaveden elektronski naslov domnevnega pošiljatelja, kamor so poslana sporočila o napakah in ostalih avtomatskih odgovorih. Če uporabnikova domena uporablja sistem SPF in ima določene svoje legitimne izvorne naslove IP, lahko prejemniki zavrnejo ponaredke s preverjanjem SPF. S tem se omeji obsežna količina povratnih sporočil, ki so posledica razpošiljanja neželene pošte.

Zapis SPF v sistemu DNS dovoljuje drugim poštnim strežnikom uporabo SPF filtriranja. Zaščitijo se pred dohodno elektronsko pošto z lažnimi ali ponarejenimi elektronskimi naslovi, povezanimi z neko domeno. Lastnikom domen pa prepreči slab ugled njihovega domenskega imena in zmanjša možnost omembe njihove domene na črnih seznamih. Za zagotovljeno delovanje morata SPF mehanizem uporabiti oba, pošiljatelj in prejemnik. Pošiljatelj objavi zapis SPF za domensko ime v DNS, prejemnik pa mora omogočiti mehanizem, ki te domenske zapise preveri in izvede ustrezne ukrepe.

4.1.1 Komponente zapisa SPF

Zapis SPF se začne s številko verzije mehanizma SPF, ki zapis TXT določi kot zapis SPF. Sledijo ji nizi predpon, mehanizmov in ponekod informatorjev. Pri preverjanju se najprej ocenijo vsi mehanizmi in predpone, nato pa še vsi informatorji. Seznam komponent je prikazan v Tabeli 4.1 [23]. Generičen zapis SPF je sledečega formata:

```
verzija ([predpona] mehanizmi)(informatorji)
```

Komponente	Opis
`Verzija:` `v=spf1`	Določa zapis TXT z uporabo SPF verzije 1.
`Predpone:` `+, -, ~, ?`	Stojijo pred mehanizmi, privzame se »+«.
`Mehanizmi:` `all, include, a, mx, ptr, ip4, ip6, exists`	Uporabi se enega ali več v nizu zapisa.
`Informatorji:` `exp, redirect`	Uporabi se do dva v nizu zapisa.

Tabela 4.1: Seznam komponent zapisa SPF.

Predpone SPF

Predpone (angl. *qualifiers*) določijo, kateri naslovi IP uspešno prestanejo test poizvedbe SPF. Vsak mehanizem se lahko kombinira z eno izmed štirih predpon, naštetih v Tabeli 4.2 [23].

PREDPONA	REZULTAT	AKCIJA
+	pass	sporočilo je sprejeto
-	fail	sporočilo mora biti zavrnjeno
~	softfail	sporočila so ponavadi sprejeta, vendar označena
?	neutral	interpretiran kot »none« (ni pravila), glej Poglavje 4.1.1

Tabela 4.2: Predpone SPF.

Mehanizmi SPF

V sklopu zapisa SPF se lahko definira od nič do osem mehanizmov. Mehanizmi opredeljujejo naslove IP, ki so avtorizirani za pošiljanje elektronske pošte iz določene domene. Ponavadi vsebujejo znake »:« ali »/« za imenom, ter so občutljivi na velikost črk. Ocenjeni so po vrstnem redu, od leve proti desni. Vsak ocenjeni mehanizem se lahko ujema, ne ujema ali vrne izjemo.

all - Deluje kot test in se vedno ujema z lokalnimi in oddaljenimi naslovi IP. Uporabi se kot skrajno desni mehanizem v zapisu, da je eksplicitno privzet. Mehanizmi, ki so zapisani za njim, ne bodo testirani.

a - Preverjanje je uspešno, če ima domena zapis A ali AAAA, ki se lahko razreši v enega izmed ciljnih naslovov IP.

ip4 - Preverja, če dano omrežje vsebuje naslov IPv4.

ip6 - Preverja, če dano omrežje vsebuje naslov IPv6.

mx - Ujemanje imamo, če je IP eden izmed gostiteljev MX za to domeno.

ptr - Testira se obstoj ustrezne reverzne DNS preslikave. Uporaba tega mehanizma se odsvetuje, ker ni povsem zanesljiv v primeru napak DNS.

include - Določi druge avtorizirane domene. Vse, kar je legitimno za podano domeno, je tudi za nas. Praviloma se uporablja, da vključi pravila več kot enega internetnega ponudnika storitve.

exists - Uporablja se za poljubno domensko ime, nad katerim se izvede poizvedba zapisa A v DNS. Najden zapis vrne ujemanje. Skupaj s SPF makro jezikom dovoljuje zapletene sheme, kot so npr. poizvedbe DNSBL (črni seznami). [23]

Listing 4.1: Primer zapisa SPF.

```
snupi.si IN TXT "v=spf1 +mx +a +a:1.2.3.4 +a:5.6.7.8 -all"
```

Če si pogledamo primer v Listing 4.1, nam ta pove, da bo preverjanje SPF uspešno (rezultat `pass`), če bo elektronsko sporočilo, naslovljeno z domeno `snupi.si`, prišlo iz trenutnega glavnega naslova IP te domene (kamor kaže zapis A), iz naslovov IP 1.2.3.4 oz. 5.6.7.8, ali pa bo IP predstavljal gostitelja MX. Pri tem se predpona `+` lahko izpusti, ker je določena že kot privzeta. Mehanizem `all` s predpono `-` pa določa, da bo zapis za vse ostale pošiljatelje s to domeno vrnil rezultat `fail`. Na Sliki 4.1 lahko vidimo, da je odhodni strežnik avtoriziran za pošiljanje sporočil z domeno `snupi.si`.

Informatorji SPF

Informatorji (angl. *modifiers*) so pari imen in vrednosti, ki ponujajo dodatne informacije poizvedb SPF. Načeloma se lahko pojavijo kjerkoli v zapisu, vendar je priporočeno, da stojijo na koncu, za vsemi mehanizmi. Vedno vsebujejo znak `=`, ki ločuje ime in vrednost. Možno je definirati dva informatorja, ki sta se širše uvedla, vsak pa se lahko pojavi le enkrat:

exp Če poizvedba SPF vrne rezultat `fail`, ta informator z uporabo makro jezika v kodo SMTP napake doda razlago, tipično je to URL.

redirect Uporabi se lahko namesto mehanizma `all` tako, da kaže na zapis pravila druge domene, kamor se nato pošlje poizvedba. Ta informator je preprostejši

za razumevanje, kot nekoliko podoben mehanizem `include`. Zapis SPF za domensko ime, ki je podano v Listing 4.2, nadomesti zapis SPF za trenutno domeno. Uporaben je za tiste, ki želijo uporabljati isti zapis za več domen. [23]

Listing 4.2: Primer zapisa SPF.

```
snupi.si IN TXT "v=spf1 redirect=abc.si"
abc.si IN TXT "v=spf1 a ~all"
```

V tem primeru se preveri zapis A domene `abc.si`. Če se ta ujema z naslovom IP pošiljajočega strežnika, zapis vrne rezultat `pass`. V nasprotnem primeru dobimo rezultat `softfail`.

Ocenjevalni rezultati

Pri ocenjevanju prejetih elektronskih sporočil, katerih domene uporabljajo zapis SPF, lahko kot rezultat poizvedbe SPF dobimo več možnih rezultatov. Nekatere izmed njih smo že spoznali v Tabeli 4.2, tu pa so poleg njih dodani še ostali rezultati s podrobnejšim opisom njihovega pomena.

Pass Odjemalec je avtoriziran, da se predstavlja z dano identiteto. Domena se obravnava kot odgovorno za pošiljanje sporočila. Nadaljnja preverjanja pravil lahko v tem primeru nadaljujejo z zaupanjem v legitimno uporabo identitete.

Fail Odjemalec ni avtoriziran za uporabo domene v dani identiteti. Preverjajoča programska oprema lahko na podlagi tega označi sporočilo ali pa ga zavrne. V sporočilo se vstavi polje `X-Header`, ki ponazarja, da je bilo sporočilo s filtrom neželene pošte zaznano kot ponarejeno.

Softfail Domena predvideva, da gostitelj ni avtoriziran, ampak ni pripravljena sprejeti stoodstotne trditve. Sporočila se na podlagi tega rezultata ne bi smelo zavrniti, se pa priporoča nadaljnje preverjanje.

Neutral Nosilci domene so izrecno navedli, da ne morejo ali ne želijo trditi ali je naslov IP avtoriziran. Obravnavan je povsem enako kot rezultat `none`.

Temperror Ta rezultat pomeni, da je SPF odjemalec naletel na začasno napako med preverjanjem ujemanja in je ni mogel pravilno interpretirati. Pojavi se lahko v primeru, da imamo nepravilen zapis DNS, da domena ne obstaja ali strežnik DNS ni dosegljiv. Mehanizem za preverjanje lahko tako sporočilo sprejme ali začasno zavrne.

Permerror Zapisi objavljene domene ne morejo biti pravilno interpretirani. To nakazuje na stanje napake, ki za razrešitev zahteva ročen poseg.

None Za domeno ni objavljenih zapisov SPF ali domena pošiljatelja, ki se preverja, ne more biti določena z dano identiteto. Preverjajoča programska oprema ne more ugotoviti ali je gostitelj odjemalca avtoriziran. [23]

4.1.2 Ranljivosti SPF

Avtentikacijski mehanizem SPF lahko privede do neželenih rezultatov in ni stoodstotno zanesljiv. V nadaljevanju opisujemo nekaj najpogostejših ranljivosti tega mehanizma.

V primeru, da uporabnik pošlje elektronsko sporočilo iz naprave, kjer so nastavljeni tuji strežniki SMTP za odhodno pošto, ki v zapisu SPF niso zavedeni, lahko poštni strežnik blokira vso elektronsko pošto, ki ne izvira iz znanih naslovov in s tem omeji nekaj svojih uporabnikov. Primer je prikazan na Sliki 4.1. SPF je neuspešen tudi pri običajnem posredovanju sporočila, kjer naslov IP odhodnega strežnika ne ustreza naslovom IP v zapisu SPF. Polje `Return-Path` namreč v teh primerih ostane enako, kar lahko blokira dostavo. Tu so izjema poštni seznami, kjer se to polje ustrezno spremeni. Rešitev je pošiljanje z avtentikacijo SMTP preko svojega strežnikka (SASL).

Druga težava se pojavi, kadar imajo pošiljatelji neželene elektronske pošte svoj račun na danem poštnem strežniku, ali če znotraj njegove domene zlorabijo okvarjen sistem. Preverjanje za to domeno namreč vrne rezultat `pass` (glej 4.1.1). Rešitve so v bolj zahtevnih implementacijah, kjer lahko nosilec domene določi različna pravila za vsakega uporabnika posebej s pomočjo SPF makro jezika, ki se nanaša na lokalni del ali preprosto zahteva, da vse poštne navedbe za domeno uporabijo avtentikacijo SMTP.

Dodatno nevarnost predstavljajo zapisi SPF z uporabo široke maske na veljavnem naslovu strežnika, ker lahko zmanjša oceno neželenih sporočil. Katera koli tovrstna pošta iz omrežja robotskih računalnikov (angl. *botnet*) posledično postane SPF veljavna, zato naraste tudi verjetnost, da pride uspešno skozi filtre neželene pošte.

Lastniki domen, ki za svojo domensko ime uporabljajo zapis SPF, morajo sprejeti tveganje, da so lahko njihova legitimna sporočila zavrnjena ali označena kot neželena pošta. To lahko preprečijo z ustreznim testiranjem in z uporabo blažje politike, npr. `softfail` (glej 4.1.1), in šele nato po potrebi določijo strožjo politiko.

4.1.3 Statistični podatki uporabe SPF

Podatki večjega ponudnika elektronske pošte v Sloveniji so pokazali, da je leta 2013 okoli 12,2% vseh dohodnih sporočil uporabljalo mehanizem SPF.

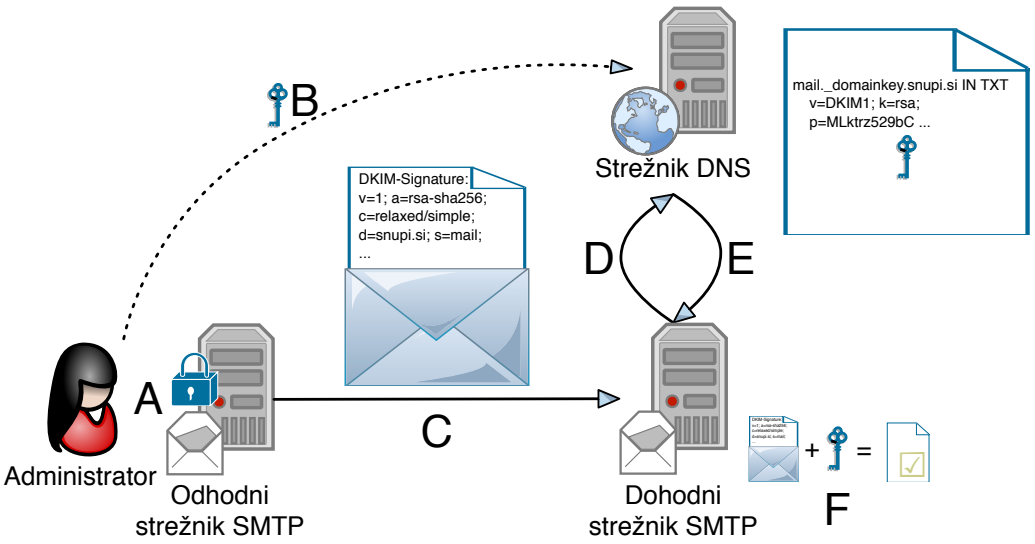
4.2 Elektronska pošta identificirana z domenskimi ključi

DKIM (angl. *DomainKey Identified Mail*) je oblika avtentikacije elektronske pošte, ki sporočilu doda identifikator domenskega imena in povečuje njegovo odgovornost v primeru neželene pošto. Bil je razvit, podobno kot pri SPF, z namenom zmanjšanja ponarejanja elektronske pošte in je nadomestil opuščeni sistem avtentikacije »DomainKeys«. Prvič je bil objavljen leta 2006, danes pa ga definira standard RFC 6376 [24].

Pomembna lastnost sistema DKIM je združljivost z obstoječo poštno infrastrukturo in se ga implementira neodvisno od odjemalcev. Rešuje tudi nekatere probleme, ki jih SPF ne more, npr. posredovanje elektronske pošte. Poleg telesa, zavaruje tudi glavo sporočila.

DKIM uporablja kriptografijo javnega ključa (glej Poglavje 2.3). S tem uporabnikom zagotavlja avtentičnost in dovoljuje preverjanje celovitosti sporočila. Delovanje DKIM, opisano v nadaljevanju, je prikazano na Sliki 4.2.

Administrator poštnega strežnika najprej generira par ključev (javnega in zasebnega), ki se bosta uporabljala za podpisovanje in preverjanje sporočil. Pri tem zasebni ključ namesti na podpisujoči odhodni strežnik (A), javni ključ pa objavi v sistem DNS (B). Ključa lahko nato uporabi za DKIM podpisovanje elektronskih sporočil. Pred pošiljanjem sporočila odhodni poštni strežnik uporabi zasebni ključ za ustvarjanje digitalnega podpisa, ki pokriva glavo in telo sporočila. Ta podpis se nato pripne sporočilu kot dodatno polje v glavi in je ločen od same vsebine sporočila. Imenuje se DKIM-podpis (angl. *DKIM-signature*). Tako podpisano sporočilo se nato pošlje do prejemnikovega dohodnega strežnika (C). Ko ta prejme sporočilo s podpisom DKIM, pošlje poizvedbo za zavedeno pošiljajočo domeno (`snupi.si`) do strežnika DNS (D). Tu pridobi javni domenski ključ, s katerim preveri ali je DKIM-podpis veljaven (E). Veljavnost podpisa dokazuje, da je bilo sporočilo podpisano s strani avtoriziranega uporabnika in da njegova vsebina med prenosom ni bila spremenjena (F) [34].



Slika 4.2: Delovanje avtentikacijskega mehanizma DKIM.

4.2.1 Kanonikalizacija

Med prenosom lahko pride do spremembe elektronskega sporočila, kar lahko povzroči neveljaven DKIM-podpis. Zaradi različnih zahtev podpisovalcev se v ta namen uporabljajo kanonikalizacijski algoritmi, ki dovoljujejo različne spremembe glave in vsebine sporočila. Pri teh algoritmih gre pravzaprav za proces pretvarjanja podatkov z več kot eno možno predstavitvijo, v neko standardno obliko, s čimer zagotovimo skladnost podatkov. Tako oblikovani podatki so nato pripravljeni na podpisovanje oz. preverjanje podpisa [35].

Poznamo dve metodi, preprosto kanonikalizacijo (angl. *simple canonicalization*) in sproščeno kanonikalizacijo (angl. *relaxed canonicalization*). Preprosta je bolj stroga in ne dovoljuje nič oz. zelo malo sprememb, medtem ko sproščena metoda sporočilo pred podpisovanjem in preverjanjem poenoti tako, da odstrani odvečne presledke in prazne vrstice na koncu besedila, ki jih lahko doda poštni agent.

Glava in telo sporočila sta kanonikalizirana in podpisana ločeno. Nad telesom sporočila se kanonikalizacija izvede pred računanjem zgoščene vrednosti in podpisa DKIM. Po podpisu telesa se glavi sporočila doda polje s podpisom DKIM, nato pa se tudi nad glavo sporočila izvedeta kanonikalizacija in zgoščevalna funkcija, nad čimer se izvede dodaten podpis. Ta se nato doda polju DKIM-podpisa v glavi sporočila. Ko poštni strežnik prejemnika prejme sporočilo, preverjanje izvede po obratnem postopku. Najprej preveri avtentičnost glave, zatem pa še telesa sporočila. Metodo algoritma izbere podpisovalec sporočila, privzet je preprost kanonikalizacijski algoritem [24].

4.2.2 Izbirniki

Vsako domensko ime uporabnika ali organizacije ima lahko v sistemu DNS določenih več javnih ključev oz. zapisov DKIM. To omogočajo izbirniki, s katerimi je mogoče razdeliti imenski prostor DNS. Zapis DKIM se v DNS doda kot poddomena v sledeči obliki: `izbirnik._domainkey.domena`. Izbirnik v tem zapisu identificira par ključev, `_domainkey` je stalna ključna beseda, na koncu pa sledi še podpisujoče domensko ime.

Uporaba izbirnikov je primerna iz več razlogov. Eden izmed njih je dobra varnostna praksa, ki narekuje mesečno ali letno spreminjanje ključa. Pri tem je prehod na nov ključ z drugim izbirnikom povsem neopazen, saj v prehodnem obdobju delujeta oba ključa. Dodaten razlog je ločen nadzor nad podpisi med različnimi oddelki oz. posameznimi uporabniki. Nekatere domene želijo imeti podpis DKIM le za določen čas, npr. za oglaševanje. Prav pridejo tudi pri zunanjem izvajanju podjetij (angl. *outsourcing*), ki uporabljajo poštne storitve v imenu druge organizacije. Po koncu uporabe ali ob morebitni ogroženosti ključa, se tak izbirnik preprosto izbriše.

4.2.3 DKIM-podpis

Podpis sporočila je shranjen v polju glave z imenom `DKIM-signature` (primer v Listing 4.3). To polje vsebuje celoten podpis skupaj s podatki za pridobivanje javnega ključa. Celotno polje je zapisano v obliki `oznaka=vrednost`. Oznake polja glave DKIM-podpisa z opisi pripadajočih vrednosti prikazuje Tabela 4.3 [24].

Vidimo, da DKIM-podpis med drugim vsebuje tudi podatke o podpisujoči domeni (oznaka `d`), identiteti uporabnika (oznaka `i`) in času poteka podpisa (oznaka `x`). Vse te podatke narekuje standard certifikata x.509, v katerem je zapisan format certifikata, pridobljen s strani overitelja digitalnega podpisa (glej Poglavje 2.3).

Oznaka polja	Pomen vrednosti
`v`	Verzija specifikacije, ki se nanaša na zapis podpisa.
`a`	Zgoščevalni algoritem, uporabljen za generiranje podpisa. (»rsa-sha1« ali »rsa-sha256«)
`b`	Podatki podpisa.
`bh`	Zgoščevalna funkcija kanonikaliziranega telesa sporočila, omejena z oznako `l`.
`c`	Kanonikalizacija sporočila. (glava/telo)
`d`	Podpisujoča domena(SDID), ki prevzema odgovornost za uvedbo sporočila v poštni tok.
`h`	Seznam podpisanih polj glave.
`i`	Dodatne informacije o identiteti uporabnika oz. agenta, v imenu katerega SDID prevzema odgovornost.
`l`	Merjenje dolžine telesa sporočila.
`q`	Ločevalni seznam poizvedbenih metod, uporabljen za obnovo javnega ključa.
`s`	Izbirnik razčlenjuje imenski prostor za oznako `d`.
`t`	Časovni žig podpisa.
`x`	Konec veljavnosti podpisa.
`z`	Kopirana polja glave.

Tabela 4.3: Oznake polja glave DKIM-podpisa.

Listing 4.3: Primer DKIM-podpisa elektronskega sporočila.

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=snupi.si;
s=mail; t=1409670682; r=y;
bh=YiPuor0x93cmcBI8kuym1+McHzXPUFUSXnjevNtEHlo=;
h=Date:From:To:Subject;
b=XreFolXY...
```

4.2.4 Zapis DKIM v DNS

DKIM uporablja zapis vira TXT za shranjevanje podatkov v DNS. Izvedeli smo že, da je teh zapisov za posamezno domensko ime lahko več, kar nam omogočajo izbirniki.

Glavna vloga zapisa DKIM v istemu DNS je, da ponudi javni ključ, ki je tako dostopen vsem in se bo uporabil pri avtentikaciji prejetega sporočila za določeno domeno in izbirnik. Prejemnikov poštni strežnik dobi celotno ime za poizvedbo DNS z izborom vrednosti, ki so vsebovane v polju glave DKIM-podpisa. Primer zapisa vidimo v Listing 4.4. Prva je vrednost polja izbirnika `s=`, sledi stalno ime `_domainkey` in nato še vrednost domene v polju `d=`. Če imamo torej domensko ime `snupi.si` ter izbirnik `mail`, se izvede poizvedba za zapis TXT `mail._domainkey.snupi.si`.

DKIM za določanje polj v DNS TXT zapisu, prav tako kot DKIM-podpis, uporablja obliko `oznaka=vrednost`. Posamezna polja so med seboj ločena s podpičjem »;«. Nekaj najpomembnejših polj zapisa DKIM v sistemu DNS je prikazanih v Tabeli 4.4 [36].

Oznaka polja	Pomen vrednosti
`v`	Verzija DKIM, edina možna in tudi privzeta je `DKIM1`.
`h`	Zgoščevalni algoritem, uporabljen za generiranje podpisa.
`k`	Algoritem javnega ključa, privzet je algoritem RSA.
`p`	Podatki javnega ključa, zapisani v obliki `base64`.

Tabela 4.4: DKIM polja zapisa TXT v sistemu DNS.

Listing 4.4: Primer zapisa DKIM v sistemu DNS.

```
mail._domainkey.snupi.si IN TXT "v=DKIM1; h=sha256; k=rsa;"
   "p=B7T8kuhgi7gVZ5tv..."
```

4.2.5 Ranljivosti DKIM

Avtentikacijski mehanizem DKIM z digitalnim podpisom doda identifikator sporočilu, kateremu lahko zaupamo in s katerim organizacija prevzema odgovornost za prenos sporočila. Zavedati se moramo, da lahko domena podpiše tudi neželena elektronska sporočila, saj mehanizem kot tak ne preverja vsebine sporočila. Skrbnik poštnega sistema mora biti zato zelo previden glede rokovanja in zaščite ključev ter dodati ustrezne filtre in ostale mehanizme, ki zaznajo neželena sporočila. DKIM ne more zagotoviti uspešne dostave sporočila in prav tako ne ponuja dokaznega gradiva o avtorstvu oz. izvoru sporočila. Te zahteve naslavljajo druge tehnologije. [37]

Pri preverjanju DKIM podpisa se v začetku uporabi storitev DNS, zato je DKIM odvisen tudi od varnosti sistema DNS. Poleg že omenjenih ranljivosti v sklopu DNS, se lahko težava pojavi med preverjanjem polja glave podpisa DKIM, kjer smo lahko pozvani k pridobivanju zapisa ključa, ki ga določi napadalec. To se zgodi na točki E, pri Sliki 4.2. Nevarnost lahko zmanjšamo tako, da si zagotovimo strogo preverjanje dodatnih informacij v odgovorih DNS. Razširjena uporaba DKIM se pokaže tudi na občutno povečanih poizvedbah DNS pri zahtevanem podpisovanju domen. Možno je tudi, da napadalec v DNS namerno objavi napačne zapise ključev, kar med preverjanjem povzroči napad DoS (glej Poglavje 3.4). Napad lahko vključuje tudi zelo veliko količino elektronske pošte, ki je poslana z uporabo lažnih podpisov od dane domene. Slednje se lahko zgodi na točki A Slike 4.2.

Pri sproščenem kanonikalizacijskem algoritmu telesa sporočila lahko pride do ASCII umetnostnega napada, kjer se v besedilo nastavljajo razmiki med besedami. Težave so lahko tudi pri sicer legitimnih sporočilih. Obstoječi standardi dovoljujejo, da vmesni strežniki MTA spremenijo vrstni red polj glave. Če podpisovalec podpiše dva ali več polj glave istega imena, lahko pride do lažne napake preverjanja. Tudi to se zgodi pri točki A Slike 4.2.

Znan je tudi napad, pri kateremu zlonamerna oseba pošilja del neželene pošte skozi MTA, ki podpisuje domeno z večjim ugledom in nato ponovno pošlje sporočilo večjemu številu prejemnikom. Ti opazijo veljaven podpis dobro poznane domene, kar dvigne njihovo zaupanje v pristnost sporočila ter s tem poveča uspešno dostavo. Napadu se lahko delno izognemo z dejstvom, da je nek elektronski naslov uporabljen za razpošiljanje neželene pošte in da so ta podpisana sporočila najverjetneje neželena. Za dovolj hiter ukrep potrebujemo mehanizem odkrivanja v realnem času. Večji preveritelji lahko zaznajo nenavadno velike količine elektronske pošte z enakim podpisom v krajši časovni periodi. Manjši pa lahko dobijo enako količino informacij skozi obstoječi skupni sistem. [24]

4.2.6 Statistični podatki uporabe DKIM

Pri večjem ponudniku elektronske pošte v Sloveniji, je bilo po podatkih vseh dohodnih DKIM-podpisanih sporočil v letu 2013 okoli 36,3%.

4.3 Domenska avtentikacija sporočil, poročanje in skladnost

Skupina vodilnih podjetij, katere močno povezuje storitev elektronske pošte (Yahoo, PayPal, Google, Microsoft, Facebook in LinkedIn), je ustvarila standard DMARC (angl. *Domain-based Message Authentication, Reporting & Conformance*) z namenom, da zapolni pomanjkljivosti že obstoječih avtentikacijskih sistemov. Želeli so doseči, da pošiljatelji objavijo preprosto politiko za ne-avtenticirana sporočila, prejemniki pa jim poročajo o rezultatih, da lahko s tem dodatno izboljšajo svoj avtentikacijski sistem.

Prvi prototip je bil izveden med podjetjema Paypal in Yahoo leta 2007, štiri leta kasneje pa so bili objavljeni prvi zapisi DMARC. V začetku leta 2012 je nato izšel prvi osnutek specifikacije DMARC. Trenutno ga definira specifikacija, ki je izšla aprila, leta 2014 [25]. Mehanizem je po enem letu zaščitil že okoli 60 odstotkov poštnih predalov uporabnikov po vsem svetu.

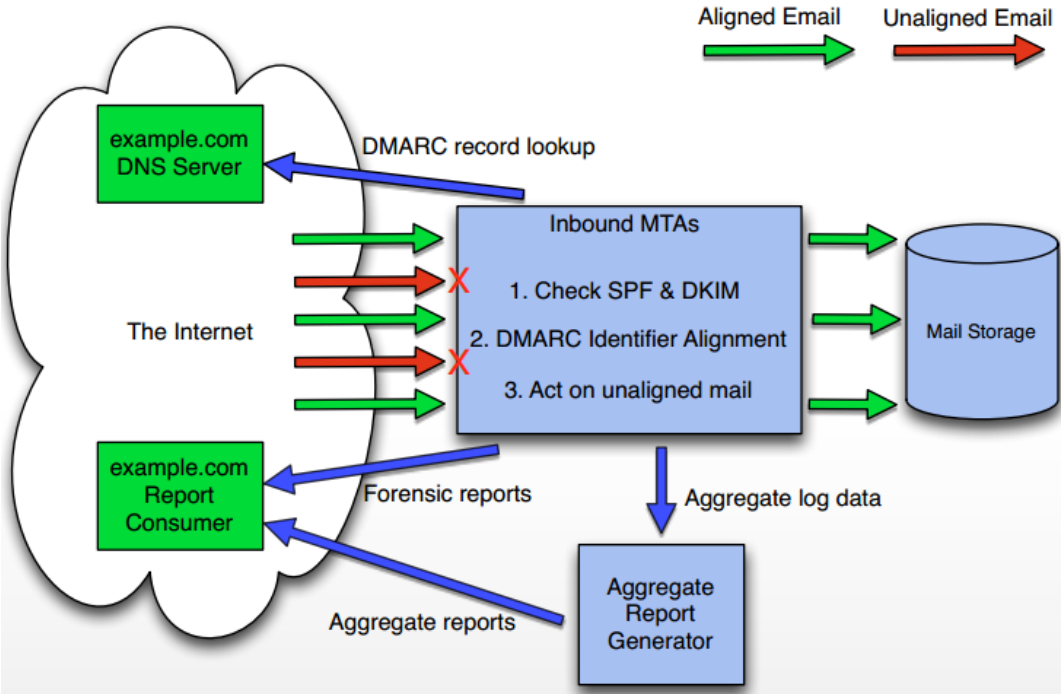
Cilj DMARC ni predstaviti nov način potrjevanja poštnih sporočil, v enakem smislu kot to počneta SPF in DKIM, ampak poenoti njuno uporabo. Kot smo spoznali do sedaj, SPF ne deluje zanesljivo, kadar je sporočilo posredovano, DKIM pa tudi ni povsem zanesljiv zaradi precej kompleksnega algoritma. Če torej uporabimo oba algoritma hkrati, s tem zmanjšamo njune slabosti.

Pri tem mehanizmu pošiljatelji in prejemniki delujejo skupaj. Pošiljatelji s posebnim DMARC zapisom TXT v sistemu DNS določijo, kako naj prejemniki ukrepajo na podlagi rezultatov mehanizmov SPF in DKIM. Na ta način lahko prejemniki omejijo potencialna neželena sporočila in pošiljatelju poročajo o rezultatih DMARC. Na podlagi teh rezultatov poročil, pošiljatelji določijo prilagodljive ukrepe politik, s katerimi omejijo lažno predstavljanje njihove domene.

DMARC predvsem ščiti večja podjetja, saj se njihova imena zelo pogosto izrablja v neželenih sporočilih. Zaradi lažnih elektronskih sporočil, ki na prvi pogled delujejo identična originalnim, namreč uporabniki bolj zaupajo v pristnost sporočila.

4.3.1 Delovanje mehanizma DMARC

Delovanje mehanizma DMARC prikazuje Slika 4.3. Zaščita se začne s podpisovanjem vseh elektronskih sporočil z DKIM in s posodobljenimi zapisi SPF, medtem ko DMARC doda še koncept poravnave identifikatorja (angl. *identifier alignment*). V nadaljevanju spoznamo, kako poteka preverjanje avtentikacije sporočila.



Slika 4.3: Delovanje mehanizma DMARC (vir slike [1]).

Različne avtentikacijske metode elektronskih sporočil ne avtenticirajo nujno istih elementov sporočila. Medtem ko DKIM avtenticira domeno, ki je sporočilu dodala podpis in je vidna pri oznaki `d=` v polju DKIM-podpisa, SPF avtenticira domeno naslova, podanega v polju `Return-Path:`. V slednjega se prenese vsebina, zavedena v `Mail from:` oz. `HELO/EHLO` (definira ju RFC 5321). Te domene so lahko različne in ni nujno, da jih uporabniki vidijo. Najbolj viden identifikator za končnega uporabnika je elektronski naslov v polju `From:` glave sporočila (definira RFC 5322), ki je običajno uporabnikom prikazan tudi kot izvorni naslov pošiljatelja. Ta identifikator za avtenticiranje uporablja mehanizem DMARC. Za lažje razumevanje si poglejmo primer v Listing 4.5, kjer imamo podano glavo sporočila:

Listing 4.5: Primer poravnave identifikatorjev.

```
Return-Path:postmaster@foo.snupi.si
Authentication-Results: mx.mail.com; spf=pass (mail.com: domain of
    postmaster@snupi.si designates 1.2.3.4 as permitted sender)
    smtp.mail=postmaster@snupi.si;
    dkim=pass header.i=@bar.snupi.si
DKIM-Signature: v=1; a=rsa-sha256; d=bar.snupi.si;
    s=s1024-2011-q2; c=relaxed/simple; q=dns/txt; i=@snupi.si;
    t=1337318096; h=From:Subject:Date:To:MIME-Version:Content-Type;
    bh=0l5o8r4ftEPBr083MbUpe0mIrWKRs5yT46DR6CGk/Mk=;
    b=T6m3ZvppP3OLGNQVoR/llW+RxSbQiRlaCcwZpXTF/xjWk0xjYl/8S0UUvtFPHZ1l
    0cy+svp5ymrqBgnDEN/ZQEcfmzYEOg1BNL/I8zlMKPmVOf/9cLIpTVbaWi/G2VBYLX
    ONpLsSymtoeqTBYOOJqoiNLzDNP01pVgZYunf8h90=;
From: "Postmaster" <postmaster@snupi.si>
```

Za posamezni mehanizem so avtenticirane domene sledeče:
SPF domena = `foo.snupi.si`
DKIM domena = `bar.snupi.si`
From domena = `snupi.si`

Poravnava identifikatorjev

DMARC lahko preveri, če je domena polju `From:` poravnana (angl. *aligned*) z identifikatorjem veljavne SPF preverbe in identifikatorjem veljavnega DKIM podpisa. Z besedo »poravnava« je mišljeno, da so vsi identifikatorji povsem enaki oz. je pod-domena organizacijske domene najdena v polju `From:`.

SPF in DKIM imata na voljo dva različna načina poravnave identifikatorjev (angl. *identifier alignment*), **strogega** (angl. *strict*) in **sproščenega** (angl. *relaxed*). Stroga poravnava zahteva točno ujemanje identifikatorjev z organizacijsko domeno, sproščena pa vključuje tudi pod-domene posameznega identifikatorja. Za vsak mehanizem se način poravnave določi ločeno, kar omogoča neodvisno dodajanje ostalih avtentikacijskih mehanizmov.

Za pozitiven rezultat DMARC preverjanja poravnave identifikatorjev, mora imeti poravnane identifikatorje vsaj eden izmed mehanizmov SPF ali DKIM. S tem se izognemo napačni obravnavi legitimnih sporočil ter pridobimo na stabilnosti in zanesljivosti mehanizma. V kolikor so vsi identifikatorji poravnani, preverjanje mehanizmov SPF in DKIM pa je neuspešno, DMARC sporočila ne smatra za poravnanega. DMARC vrne rezultat `pass`, če je sporočilo poravnano in rezultat `fail`, če ni.

Če se vrnemo k našemu primeru na Sliki **??**, vidimo da bo sporočilo poravnano, če uporabimo sproščeno poravnavo identifikatorjev za vsaj enega izmed obeh mehanizmov (SPF in DKIM). Če je njuna poravnava identifikatorjev stroga, pa bo preverjanje DMARC neuspešno. Pozorni moramo biti tudi na rezultate preverjanj posameznih mehanizmov SPF in DMARC. Ker sta oba rezultata `pass`, se lahko osredotočimo le na poravnavo identifikatorjev.

4.3.2 Zapis DMARC in vrste politik

Lastniki domen morajo za uporabo mehanizma DMARC objaviti ustrezen zapis TXT v sistemu DNS. Podobno kot pri DKIM, se zapisu doda predpona `_dmarc` pred pod-domeno, ki jo želi ponudnik elektronske pošte zaščititi. V Tabeli 4.5 [1] je seznam veljavnih polj znotraj formata zapisa DMARC z njihovimi opisi. Obvezni sta le prvi dve oznaki. [1]

komponenta	opis
`v`	Verzija protokola, katere vrednost mora biti `DMARC1`.
`p`	Pove politiko domenskega imena. Lahko je ena izmed treh možnih, naštetih v nadaljevanju.
`sp`	S to oznako se lahko zaščitijo vse pod-domene, v kolikor za določeno domeno ni pod-domen.
`pct`	Ponazarja odstotek sporočil, s katerim prejemnik sprejme določeno politiko. Če je vrednost npr. 50 in prejemnik prejme 100 sporočil iz te domene, je 50 izmed njih potencialno zavrnjenih in 50 ne.
`adkim` `aspf`	Način poravnave se obravnava posamezno za vsak avtentikacijski mehanizem. Ločeno za DKIM in SPF. Privzame se sproščena poravnava identifikatorjev.
`rua` `ruf`	Na naslove, zapisane v posamezni oznaki, se pošljejo poročila, ki jih generirajo prejemniki. Na naslov prve oznake se pošljejo skupna poročila, na naslov druge pa forenzična poročila.
`rf`	Format forenzičnega poročanja.
`ri`	Interval skupnega poročanja v minutah, ki pove, kako pogosto želimo dobivati poročila prejemnika.

Tabela 4.5: Komponente zapisa DMARC.

S komponento `p` v zapisu DMARC administrator domene določi politiko, s katero preverjajočemu dohodnemu strežniku pove, na kakšen način naj obravnava elektronska sporočila, poslana znotraj njegove domene. Sledi nekoliko podrobnejši opis posameznih vrst politik.

None Uporabi se, kadar lastnik domene pošiljatelja želi le dobivati in analizirati poročila. Prejemniki sporočil s to politiko zapisa DMARC ne glede na ugotovitve sporočila ne ukrepajo. V poročilu pa vseeno prejme rezultate ocenjevanja prejemnika, kar mu pomaga pri ustvarjanju najbolj ustreznega

zapisa DMARC za njegovo domeno.

Quarantine Ta politika obravnava sporočilo z visoko stopnjo suma, da gre za vsiljeno pošto. Kljub temu lastnik domene pošiljatelja ne želi, da prejemnik zavrne sporočilo v primeru neporavnanih identifikatorjev. Sporočila so ponavadi dostavljena v posebno mapo z neželeno pošto ali pa zadržana, uporabniku pa se pošlje obvestilo.

Reject Neporavnano elektronsko sporočilo se zavrne.

Vzemimo primer zapisa DMARC (Listing 4.6), objavljenega v sistemu DNS z zapisom TXT in ga primerjajmo s sporočilom v Listing 4.5.

Listing 4.6: Primer zapisa DMARC v sistemu DNS.

```
_dmarc.snupi.si IN TXT "v=DMARC1; p=quarantine; adkim=r; aspf=s;
   rua=mailto:rua@snupi.si"
```

Zapis določa, da ima mehanizem DKIM sproščeno, mehanizem SPF pa strogo poravnavo identifikatorjev. Za DKIM torej imamo poravnavo, pri SPF pa ne. Domena `foo.snupi.si` namreč ni enaka domeni `snupi.si`, ki je v polju `From:`. Ker je celotno sporočilo zaradi uspešne poravnave DKIM vseeno poravnano, bo rezultat DMARC testa vrnil `pass` in sporočilo bo uspešno dostavljeno v poštni predal prejemnika (če izvzamemo ostala morebitna pravila preverjanja). Recimo, da bi imeli tudi pri DKIM strogo poravnavo identifikatorjev. V tem primeru bi DMARC vrnil rezultat `fail`, sporočilo pa bi bilo dostavljeno v mapo z neželeno pošto, kar nam določa politika `quarantine`.

4.3.3 Skupna in forenzična poročila

V zapisu DMARC lahko določimo enega ali več elektronskih naslovov, na katere dobivamo poročila prejemnikov naše elektronske pošte. Skupna poročila (angl. *aggregate reports*) vsebujejo informacije o tem, koliko elektronskih sporočil s to domeno je bilo prejetih, iz katerega naslova IP prihajajo, koliko teh sporočil je bilo poravnanih in kaj je bil razlog poravnave. Opazne so lahko tudi druge pomanjkljivosti, npr. da katero izmed sporočil ni bilo podpisano z DKIM ali pa da kateri izmed legitimnih pošiljajočih MTA strežnikov ni bil dodan v zapis SPF. Te

informacije predstavljajo dober način za testiranje poštne strukture in so ključnega pomena za oblikovanje čimbolj ustreznega zapisa DMARC za posamezno domeno. Elektronski naslov prejemnika skupnih poročil podamo s komponento `rua` (angl. *reporting URI of aggregate reports*), podana je v Tabeli 4.5. Forenzična poročila (angl. *forensics reports*) ponavadi vsebujejo obnovljene verzije zavrnjenih sporočil vendar so predvsem zaradi vprašanja zasebnosti redko v uporabi. Komponenta `ruf` (angl. *reporting URI of forensic reports*), s katero podamo elektronski naslov prejemnika forenzičnih poročil, je podana v Tabeli 4.5.

Z analizo podatkov prejetih poročil lahko ocenimo količino neželene elektronske pošte oz. lažnega predstavljanja domenskega imena, gledamo naslove, ki ne prihajajo od našega ponudnika internetnih storitev (SPF ni poravnan) ali z neustreznimi podpisi DKIM. Uporaba mehanizma DMARC ni zagotavlja odpravo vse neželene elektronske pošte, lahko pa do neke mere prisili lažne pošiljatelje, da ne zlorabljajo domenskih imen, ki uporabljajo DMARC.

4.3.4 Ranljivosti DMARC

Pri implementaciji mehanizma DMARC se najprej srečamo z vprašanjem izpostavljenosti podatkov. V nasprotju z drugimi mehanizmi prejemnikom omogoča pošiljanje povratnih informacij, ki navajajo podrobnosti sporočila. Te se podane v skupnem poročilu in se nanašajo na osnovne mehanizme za preverjanje pristnosti. Forenzična poročila lahko vsebujejo tudi vsebino sporočila in sledi polj glave sporočila. DMARC prav tako dovoljuje pošiljanje poročil vmesnemu posredniku, ki deluje v imenu domene. Prejem teh podatkov s strani tretjih oseb lahko politika o zasebnosti dovoli ali ne. Zato morajo lastniki domen in prejemniki elektronske pošte temeljito pregledati in razumeti njihove notranje politike, da preverijo, če ta omejuje pogoje uporabe in prenos poročil DMARC.

Obvezno se je potrebno izogniti nešifriranim mehanizmom. Ti lahko povzročijo razkritje podatkov, poslanih v poročilu, čeprav so bili ti v sporočilu prvotno šifrirani ali kako drugače zavarovani.

Mehanizem DMARC in avtentikacijski mehanizmi, na katerih temelji, so odvisni tudi od varnosti sistema DNS. Ker forenzična poročila vsebujejo precej občutljive podatke, je parameter `ruf=` zapisa DMARC za napadalce precej atraktiven. Za zmanjšanje izpostavljenosti ranljivostim DNS, je najboljša rešitev implementacija

DNSSEC na strani lastnika domene in prejemnika.

Najbolj ranljivo točko orodja DMARC predstavlja osredotočanje na identifikator `From:` naslova, ki je del podatkov telesa sporočila. Izbira tega identifikatorja je najboljša rešitev, saj je izmed vseh ostalih identifikatorjev ta vedno prisoten. Večina MUA se osredotoča ravno nanj. Napadalci to izkoriščajo z napadom prikaznega imena. Dostikrat MUA prikaže le prikazno ime in ne elektronskega naslova, zato lahko pošiljatelji vsiljene pošte v prikazno ime dajo ime poznane znamke.

Težavo predstavlja tudi sproščena poravnava identifikatorjev, ki dovoljuje poravnavo za pod-domene. Če zlonamerna oseba dobi nadzor nad SPF zapisom ali DKIM podpisovanjem za pod-domeno, se lahko ta uporabi za generiranje pozitivnega rezultata pri mehanizmu DMARC. Rešitev je striktna poravnava identifikatorjev.

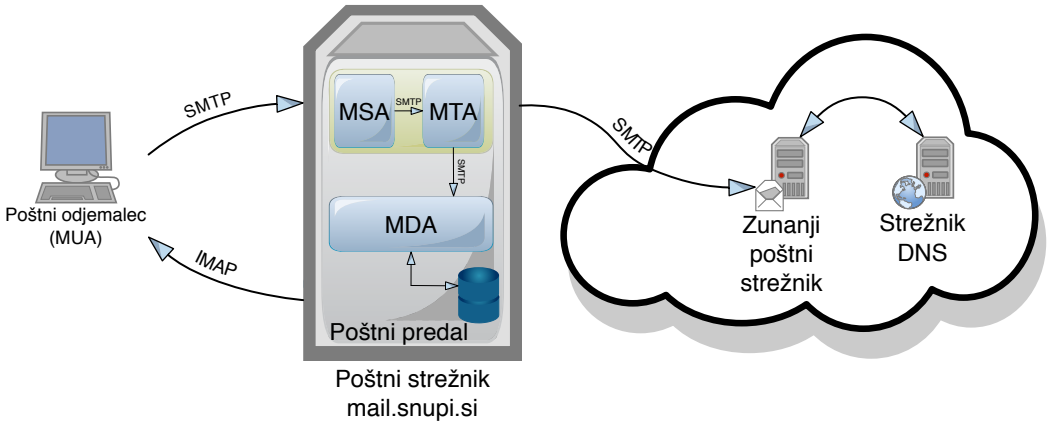
Poglavje 5

Implementacija poštnega strežnika z overovljanjem

5.1 Opis okolja

Postavili bomo poštni strežnik, ki bo deloval hkrati kot strežnik za odhodno pošto (MTA) in strežnik za dohodno pošto (MDA), kot je prikazano na Sliki 5.1. S tem bomo omogočili pošiljanje in prejemanje elektronske pošte preko našega poštnega strežnika. Za domeno, ki bo predstavljala našo identiteto, bomo dodali ustrezne zapise v sistem DNS. Vzpostavili bomo potrditveno elektronsko pošto (MSA), ter poskrbeli najprej za vzpostavitev avtentikacije SASL in nato še za varno povezavo SSL, skozi katero bo tekel šifrirani promet med poštnim odjemalcem in našim strežnikom. Tako bomo zagotovili primerno avtentikacijo SMTP. Na strežnik bomo namestili samo-podpisani digitalni certifikat, s pomočjo katerega bomo omogočili avtentičnost in celovitost podatkov.

Za avtentikacijo avtoriziranih strežnikov naše domene bomo implementirali avtentikacijski mehanizem SPF. Odhodna sporočila bomo digitalno podpisali z uporabo mehanizma DKIM, ter na koncu izvedli še implementacijo avtentikacijskega mehanizma DMARC, ki bo s pomočjo SPF in DKIM še dodatno zaščitil našo domeno.



Slika 5.1: Testno okolje.

5.2 Nastavitve

Na strežnik smo namestili operacijski sistem Ubuntu 13.10. Gre za eno izmed distibucij Debian in je bil izbran zaradi široke razširjenosti na področju strežniških sistemov. Pri postavitvi poštnega strežnika smo za MTA uporabili odprto-kodno programsko opremo Postfix, ki je že privzeta na operacijskem sistemu Ubuntu in velja za precej zmogljiv in varen sistem. Skladno s tem smo za MDA izbrali programsko opremo Dovecot, s katero se Postfix pogosto kombinira. Dodali smo tudi nekaj sistemskih uporabnikov s katerimi smo lahko preizkusili delovanje poštnega strežnika. Testiranje s strani pošiljatelja je bilo izvedeno s poštnim odjemalcem Mozilla Thunderbird, imel je vlogo MUA.

5.2.1 Nastavitve DNS

Identiteto našega poštnega strežnika je predstavljalo domensko ime `snupi.si`, v imenu katerega smo pošiljali elektronska sporočila iz našega strežnika. V sistem DNS smo dodali sledeče zapise virov, prikazane na Tabeli 7.1. Za domeno `snupi.si` in domeno, ki smo jo določili za poštni strežnik `mail.snupi.si`, smo dodali zapisa A, ki kažeta na naslov IP našega poštnega strežnika. Kadar koli se bo

za naše domensko ime izvedla poizvedba DNS, bo sistem DNS lahko našel naslov IP poštnega strežnika. Dodali smo tudi zapis MX za ime poštnega strežnika, ker se pri pošiljanju elektronske pošte vedno poizvedba izvede najprej za ta zapis in šele nato za zapis A. S tem prihranimo na času. Ker je večina poštnih strežnikov nastavljenih tako, da zavračajo prihajajočo elektronsko pošto iz naslovov IP brez urejenih zapisov PTR, smo za naš IP strežnika določili tudi tega.

5.2.2 Nastavitve Postfix

Postfix ima dve konfiguracijski datoteki:

- `main.cf` - vsebuje glavne konfiguracijske nastavitve
- `master.cf` - določa storitve, ki naj jih Postfix poganja

Najprej smo popravili konfiguracijsko datoteko `main.cf`. Končna vsebina datoteke je podana v Listing 7.1. Za ime gostitelja smo določili ime `uta.snupi.si`, ter izvor nastavili na vsebino datoteke `/etc/mailname`, kamor smo predhodno vnesli ime našega poštnega strežnika, in sicer `mail.snupi.si`. Postfix privzeto posreduje elektronska sporočila odjemalcev avtoriziranih omrežij na katero koli lokacijo. Avtorizirana omrežja so podana s parametrom `mynetworks`. Pošiljanje elektronskih sporočil smo zaenkrat dovolili le odjemalcem znotraj našega lokalnega omrežja, za ostale odjemalce bomo poskrbeli nekoliko kasneje. Nastavili smo tudi, za katere domene želimo prejemati elektronsko pošto (parameter `mydestination`). Ob tem MDA privzeto najprej vedno preveri vse prejemnike v datotekah `/etc/passwd` in `/etc/aliases`, kjer so zavedeni vsi uporabniki poštnega predala in neobstoječe zavrne. S parametrom `inet_interfaces` smo dovolili povezovanje do strežnika iz katere koli lokacije ter dodali še nekaj varnostnih omejitev glede prejemanja in pošiljanja elektronske pošte.

5.2.3 Nastavitve Dovecot

MDA smo namestili s paketi `dovecot-core dovecot-imapd`. Omogočil nam bo prejem elektronskih sporočil od MTA, naši uporabniki pa bodo lahko pridobili svoja sporočila preko protokola IMAP. Konfiguracijske datoteke za Dovecot se nahajajo na lokaciji `/etc/dovecot/`, glavno konfiguracijsko datoteko predstavlja

`dovecot.conf`. Njena vsebina je podana v Listing 7.3. Tu smo določili, da želimo uporabiti protokol IMAP, kar smo podali s parametrom `protocols`, pri čemer smo poleg `imap` določili še `imaps` za šifrirano povezavo SSL [11]. V Poglavju 2.3 smo omenili, da je najbolj običajen mehanizem golo besedilo. Parameter ki bi preprečil tovrstno avtentikacijo smo zato postavili na `no`. Sporočila se bodo nahajala na lokaciji, določeni v parametru `mail_location`, shranjena pa bodo v formatu `mbox`.

5.2.4 Nastavitev varnega dostopa

Nastavili smo že, da SMTP strežnik sprejme elektronsko pošto z oddaljenih lokacij, če je naslov IP odjemalca v istem omrežju. Za odjemalce zunaj tega omrežja pa je rešitev avtentikacija SMTP [9], ki jo podpira tudi Postfix in temelji na SASL [10]. Z uporabo tega protokola se odjemalec avtenticira MTA skozi avtentikacijski mehanizem golega besedila in obratno. Za šifriranje avtentikacijskega procesa se uporabi varna povezava TLS. Najprej smo vzpostavili avtentikacijo SASL, zatem pa še varno povezavo TLS.

Dovecot ima svojo SASL implementacijo, ki jo lahko uporabimo s Postfix. V Dovecot je bilo potrebno odpreti vtičnik, da ga lahko Postfix uporablja za avtentikacijo, glej funkcijo `service auth` v Listing 7.3.

V Postfix datoteki `main.cf` smo spremenili nastavitve na Dovecot SSL implementacijo ter dodali še nekaj ostalih potrebnih parametrov `sasl`, glej Listing 7.1.

Na koncu smo datoteko `/etc/default/saslauthd` dodali še `START=yes` in po ponovnem zagonu vseh storitev (Dovecot, Postfix, SASL) je bila avtentikacija SASL vzpostavljena.

Za vzpostavitev MUA z našim poštnim strežnikom smo onemogočili pošiljanje elektronske pošte preko vrat 25 ter omogočili le potrditvena vrata 587, ki delujejo skozi šifrirano povezavo TLS. Obenem se izognemo zavrnitvi elektronske pošte v primeru, da avtentikacijski mehanizem SASL ni dosegljiv. Popraviti smo morali nastavitve v MTA `master.cf` datoteki tako, da smo omogočili potrditev. Vsebina te datoteke je prikazana v Listing 7.2. Poleg že obstoječe storitve `smtp`, smo dodali še `submission`. Na ta način smo vzpostavili potrditveni poštni agent (MSA), ki je v našem primeru pravzaprav komponenta znotraj sistema Postfix. MSA zavaruje zunanjo povezavo tako, da preveri uporabniško ime in geslo odjemalcev, ki se povezujejo na naš strežnik.

Ko pri varnostnih nastavitvah MTA datoteke `main.cf` v parameter `smtpd_recipient_restrictions` dodamo še vrednost `permit_sasl_authenticated`, naš Postfix SMTP strežnik dovoli avtenticiranim SASL odjemalcem pošiljanje elektronske pošte na druge lokacije.

MUA, ki se bo povezoval z našim poštnim strežnikom preko povezave TLS, bo moral prepoznati certifikat uporabljen za TLS. Zadostuje, da ustvarimo samopodpisani certifikat, ki ga uporabniki nato ročno sprejmejo. Za implementacijo SSL smo uporabili orodje OpenSSL. Najprej smo morali ustvariti overitelja digitalnih potrdil, s katerim smo nato podpisali certifikat.

Z naslednjim procesom smo generirali 2048-bitni zasebni ključ, ki se je uporabil za kreiranje javnega certifikata overitelja v formatu PEM. S tem certifikatom overitelja nato podpisujemo druge certifikate. Veljavnost našega certifikata bo 730 dni.

```
root@uta:/etc/pki# openssl req -x509 -newkey rsa:2048 -out
    cacert.pem -outform PEM -days 730
Generating a 2048 bit RSA private key
...................+++
writing new private key to 'privkey.pem'
-----
Country Name (2 letter code) [AU]:SI
State or Province Name (full name) [Some-State]:Ljubljana
Locality Name (eg, city) []:Ljubljana
Organization Name (eg, company) []:Snupi Mail
Organizational Unit Name (eg, section) []:SM
Common Name (e.g. server FQDN or YOUR name) []:mail.snupi.si
Email Address []:alenka.turk.13@gmail.com
```

```
[ CA_default ]
dir = /etc/pki/             #mapa, kjer imamo vse shranjeno
database = $dir/CA/index.txt #indeks datoteka podatkovne baze
serial = $dir/CA/serial     #trenutna serijska stevilka
new_certs_dir = $dir/newcerts #privzeto mesto za nove certifikate
certs = $dir/certs           #mapa z izdanimi certifikati
```

```
certificate = $dir/certs/cacert.pem #javni certifikat overitelja
private_key = $dir/private/cakey.pem #zasebni kljuc overitelja
```

Na strežniku smo generirali zasebni ključ in zahtevek CSR z javnim ključem. Za zasebni ključ smo uporabili šifrirni algoritem DES s ključem dolžine 2048 bitov. Uporabili smo sledeči ukaz:

```
openssl genrsa -des3 -out mail.snupi.si.key 2048
```

Če strežniški ključ pustimo zaščiten z geslom, ga bo potrebno ročno vnesti vsakič, ko se zažene strežniška aplikacija z uporabo šifriranega ključa. To predstavlja problem v primeru nepravilnega zagona strežnika, iz tega razloga smo raje uporabili nešifriran ključ. V ta namen smo izvedli naslednje ukaze:

```
openssl rsa -in mail.snupi.si.key -out mail.snupi.si.key.insecure
mv mail.snupi.si.key mail.snupi.si.key.secure
mv mail.snupi.si.key.insecure mail.snupi.si.key
```

Nešifrirani ključ se sedaj imenuje `mail.snupi.si.key`. Ta datoteko lahko uporabimo za generiranje CSR brez gesla. CSR ali zahtevek za podpisovanje certifikata je blok šifriranega besedila, ki je generiran na strežniku, kjer bo certifikat uporabljan. Vsebuje informacije, ki bodo vključene v certifikat, kot je ime organizacije, domensko ime, kraj in država. Sestavlja ga tudi javni ključ, ki bo del certifikata. Zasebni ključ je običajno kreiran isti čas, kot ustvarimo CSR. Overitelj bo uporabil CSR, da bo ustvaril naš certifikat, zasebni ključ pa moramo obdržati kot skrivnost. Ustvarjen certifikat z določenim CSR bo deloval le s zasebnim ključem, s katerim je bil generiran. Z uporabo zasebnega ključa, ki je vsebovan v datoteki `mail.snupi.si.key`, smo ustvarili nov zahtevek:

```
openssl req -new -key mail.snupi.si.key -out mail.snupi.si.csr
```

Datoteko CSR smo poslali za procesiranje k svojemu CA, ki smo ga prej ustvarili. Ta je zavedene informacije preveril in nam izdal certifikat:

```
openssl x509 -req -days 730 -in mail.snupi.si.csr -signkey
   mail.snupi.si.key -out mail.snupi.si.crt
Signature ok
subject=/C=SI/ST=Ljubljana/L=Ljubljana/O=Snupi Mail/OU=SM/
CN=uta.snupi.si/emailAddress=alenka.turk.13@gmail.com
Getting Private key
```

Po prejemu certifikata smo ga namestili na strežnik in tako omogočili varno povezavo SSL na našem poštnem strežniku:

```
cp mail.snupi.si.key private/
mv mail.snupi.si.crt mail.snupi.si.crt.selfsign
```

Certifikat in ključ dodamo še v Dovecot ter zahtevamo uporabo povezave SSL, v Listing 7.3 lahko ta polja vidimo pod oznako `ssl`. V MTA nastavimo ustrezne poti do certifikata in njegovega ključa ter omogočimo šifriranje TLS za dohodno in odhodno pošto s čimer je naš Postfix konfiguriran za avtentikacijo SMTP. Polja z oznako `tls` v Listing 7.1 prikazujejo potrebne nastavitve.

5.3 Implementacija SPF

Po uspešni konfiguraciji poštnega strežnika smo nadaljevali z implementacijo avtentikacijskih mehanizmov. Programsko opremo za SPF smo namestili s paketom `postfix-policyd-spf-python`. Za integracijo z MTA smo v konfiguracijsko datoteko Postfix `master.cf` dodali zapis z oznako `policyd-spf`, prikazan v Listing 7.2. Ta zapis ustvari storitev, ki posluša preko domenskega vtičnika. Implementira jo demon Postfix z izvrševanjem programa politike strežnika (angl. *policy server*), določenega z argumentom `argv` in pravicami atributa `user`.

Potrebno je bilo ustvariti še pravila za SPF v glavni konfiguracijski datoteki storitve Postfix, glej Listing 7.1. Dopisali smo jih k že obstoječemu parametru z omejitvami prejemanja elektronske pošte, `smtpd_recipient_restrictions`. Časovno omejitev smo dodali v izogib prekinitvi, medtem ko se sporočilo še procesira.

Dodatne nastavitve SPF se lahko nastavlja v konfiguracijski datoteki, ki se nahaja na `/etc/postfix-policyd-spf-python/policyd-spf.conf`.

Na koncu je bilo seveda v sistem DNS potrebno dodati ustrezen SPF TXT zapis. Ker se elektronska pošta z našo domeno »snupi.si« pošilja iz enega strežnika, lahko dodamo precej preprost zapis SPF, ki dovoljuje pošiljanje elektronske pošte le iz naslova IP našega poštnega strežnika (Listing 5.1).

Listing 5.1: DNS TXT zapis za SPF.

```
v=spf1 mx a ip4:194.249.58.26 -all
```

Dodan zapis nam pove, da bo elektronska pošta, poslana v imenu naše domene, uspešno prestala preverjanje mehanizma SPF le, če so izpolnjeni naslednji pogoji:

- ima domensko ime MX in A zapis, ki se razreši v naslov pošiljatelja
- je naslov IP pošiljajočega strežnika IPv4 194.249.58.26

Ko pošljemo sporočilo iz našega poštnega strežnika, lahko v izvorni kodi sporočila prejemnika vidimo pozitiven rezultat SPF:

```
Received-SPF: pass (google.com: domain of alenka@snupi.si
   designates 194.249.58.26 as permitted sender)
   client-ip=194.249.58.26;
```

5.4 Implementacija DKIM

Za digitalno podpisovanje DKIM vseh odhodnih elektronskih sporočil smo na naš poštni strežnik namestili DKIM paket `opendkim`. Opendkim je odprto-kodna implementacija avtentikacijskega sistema DKIM.

Za začetek smo generirali javni in zasebni ključ (glej Listing 5.2), ki se bo uporabil za podpisovanje vseh odhodnih sporočil ter hkrati določili ime izbirnika `snmail` s stikalom `-s`. Z uporabo stikala `-d` smo tudi tokrat uporabili domensko ime `snupi.si`. Za dolžino ključa se uporabi privzeta vrednost, kar znaša 1024 bit.

Listing 5.2: Generiranje javnega in zasebnega ključa.

```
opendkim-genkey -s snmail -d snupi.si
```

Ukaz na Listing 5.2 generira dve datoteki, `snmail.private`, naš zasebni ključ ter `snmail.txt`, kjer je zapisan javni ključ. Privatni ključ smo shranili v mapo `mail` pod imenom `dkim.key`, v sistem DNS pa dodali zapis TXT s pod-domeno `snmail._domainkey.snupi.si`, ki je kombinacija izbirnika in domene. V parameter `p=` tega zapisa smo vnesli vsebino datoteke z javnim ključem.

Listing 5.3: Zapis TXT z DKIM.

```
snmail._domainkey     IN      TXT     ( "v=DKIM1; k=rsa;"
"p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCbdMZ0c2YarP4Gm40niEAlvK
P4IU2XccFM1Efol/orBsehBF3k7kLmELqrnNvjVCaY7q52bgSy5DM8TkW1NiqPd5l
0Ml1S+EXsbpuztsQl4ZWt0WewNwqh9+3WGz+8BFCeGTGzgAMeWKakNQ2Vmjd3ilKt
2UCwY92HyvYgKe4CMwIDAQAB" ) ; ----- DKIM key snmail for snupi.si
```

V konfiguracijski datoteki `opendkim.conf` je bilo potrebno nastaviti še ustrezne parametre. Vsebina te datoteke je vidna v Listing 7.4. Podali smo ime naše domene, lokacijo privatnega ključa, izbran izbirnik in določili kanonikalizacijska algoritma za glavo in telo sporočila.

OpenDKIM uporablja tudi konfiguracijsko datoteko, locirano na datotečnem sistemu `/etc/default/opendkim`. Ta datoteka se uporablja zato, da lahko MTA (Postfix) komunicira z DKIM ter s tem omogoča podpisovanje odhodnih elektronskih sporočil. Nastavili smo, da se lahko z njim poveže preko vtičnika 8891, kot prikazano v Listing 5.4.

Listing 5.4: Generiranje javnega in zasebnega ključa.

```
SOCKET="inet:8891@localhost"
```

Ustrezne parametre je potrebno dodati še v Postfix datoteko `main.cf`, glej oznako `milter` v Listing 7.1.

Testiranje pravilno nastavljenega mehanizma izvedemo preprosto z ukazom `dig snmail._domainkey.snupi.si TXT`, ki nam vrne zapis TXT. Sporočila, ki se sedaj pošiljajo iz našega poštnega strežnika, so podpisana z digitalnim certifikatom.

5.5 Implementacija DMARC

Implementacija DMARC se začne z namestitvijo paketa `opendmarc` in uporablja konfiguracijsko datoteko `opendmarc.conf`. Podobno kot pri DKIM, smo tudi tukaj nastavili povezavo med DMARC in Postfix, tokrat z vtičnikom 8893. Po dodanem vtičniku v datoteko `main.cf` poleg `milter_dkim`, dodamo še `milter_dmarc` (glej Listing 7.1).

V sistem DNS smo vnesli zapis za DMARC v pravilni obliki (glej Listing 5.5). DMARC ob začetku implementacije predvideva testiranje in zbiranje informacij s pomočjo poročil prejemnikov. Zato smo tudi za naš zapis določili politiko `none` ter elektronski naslov, kamor bomo dobivali skupna in morebitna forenzična poročila. Ta sporočila lahko dobimo s strani ponudnikov, ki tudi sami uporabljajo DMARC. Ker naš poštni strežnik uporablja le elektronske naslove z domeno »snupi.si«, smo dodali tudi parameter `sp=` in z njegovo vrednostjo določili zavrnitev vseh sporočil, poslanih iz katere koli pod-domene.

Listing 5.5: Zapis za DMARC v TXT DNS.

```
_dmarc.snupi.si. IN TXT "v=DMARC1; p=none; sp=reject ;
    rua=mailto:dmarc-rua@snupi.si; ruf=mailto:dmarc-ruf@snupi.si;
    ri=3600"
```

Če sedaj pošljemo še eno testno sporočilo, opazimo dodatno polje, tokrat z rezultati DMARC (Listing 5.6).

Listing 5.6: Avtentikacijski rezultati prejetega sporočila.

```
Authentication-Results: mx.google.com;
spf=pass (google.com: domain of alenka@snupi.si designates
    194.249.58.26 as permitted sender) smtp.mail=alenka@snupi.si;
dkim=pass header.i=@snupi.si;
dmarc=pass (p=NONE dis=NONE) header.from=snupi.si
```

Poglavje 6

Testiranje DMARC

Testiranje smo izvedli s pomočjo testnega strežnika (*mail.arnes.si*), preko katerega smo pošiljali sporočila s pomočjo protokola Telnet, ki omogoča vzpostavitev povezave z oddaljeno napravo. Povezali smo se preko vrat 25, torej za uspešno pošiljanje nismo potrebovali uporabniškega imena in gesla. Za povezavo smo v ukazno vrstico CMD (angl. *command prompt*) vnesli ukaz `telnet mail.arnes.si 25` in nato generirali sporočilo z znanimi ukazi SMTP (glej Poglavje 2.5.4). Tak postopek smo uporabili tudi za vsa nadaljnja testiranja, omenjena v tem poglavju.

Prikaz generiranega sporočila je viden v Listing 6.1.

Listing 6.1: Testno sporočilo, poslano preko Telneta.

```
220 mail.arnes.si ESMTP Postfix
MAIL FROM: alenka@snupi.si
250 2.1.0 Ok
RCPT TO: alenka.turk.13@gmail.com
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Subject: Test
Testno sporocilo.
Lp, A
.
250 2.0.0 Ok: queued as 5B6F27206E3
```

Kot vidimo, je bilo sporočilo uspešno poslano iz elektronskega naslova `alenka@snupi.si`, na naslov `alenka.turk.13@gmail.com`. Tukaj je pomembno omeniti, da smo za prejemnika izbrali elektronski naslov ponudnika elektronske pošte Google (z domeno `gmail.com`), ker uporablja in preverja vse avtentikacijske mehanizme, ki jih obravnavamo v naši diplomski nalogi. To je pogoj za uspešno testiranje.

6.1 Testiranje mehanizma SPF

Najprej smo izvedli testiranje različnih predpon zapisa za mehanizem SPF. Zanimalo nas je, če ima sporočilo, poslano iz ne-avtoriziranega strežnika, ustrezen rezultat preverjanja. Pri predponi `+all` (Listing 6.2), smo dobili povsem enak rezultat, kot pri poslanemu sporočilu iz avtoriziranega strežnika. Predpona namreč narekuje, da je kateremu koli strežniku dovoljeno pošiljanje sporočila z domeno »snupi.si«.

Listing 6.2: Predpona +all.

```
Received-SPF: pass (google.com: domain of alenka@snupi.si
   designates 193.2.1.74 as permitted sender) client-ip=193.2.1.74;
```

Mehanizem SPF je imel pri vseh ostalih predponah (`-all` (Listing 6.3), `~all` (Listing 6.4), `?all` (Listing 6.5)) negativne rezultate.

Listing 6.3: Predpona -all.

```
Received-SPF: fail (google.com: domain of alenka@snupi.si does not
   designate 2001:1470:8000::74 as permitted sender)
   client-ip=2001:1470:8000::74;
Authentication-Results: mx.google.com;
spf=hardfail (google.com: domain of alenka@snupi.si does not
   designate 2001:1470:8000::74 as permitted sender)
   smtp.mail=alenka@snupi.si;
```

Listing 6.4: Predpona ∼all.

```
Received-SPF: softfail (google.com: domain of transitioning
    alenka@snupi.si does not designate 193.2.1.74 as permitted
    sender) client-ip=193.2.1.74;
Authentication-Results: mx.google.com;
spf=softfail (google.com: domain of transitioning alenka@snupi.si
    does not designate 193.2.1.74 as permitted sender)
    smtp.mail=alenka@snupi.si;
```

Listing 6.5: Predpona ?all.

```
Received-SPF: neutral (google.com: 193.2.1.74 is neither permitted
    nor denied by domain of alenka@snupi.si) client-ip=193.2.1.74;
Authentication-Results: mx.google.com;
spf=neutral (google.com: 193.2.1.74 is neither permitted nor
    denied by domain of alenka@snupi.si) smtp.mail=alenka@snupi.si;
```

Testirali smo tudi navadno posredovanje sporočila, kar je po predvidevanjih povzročilo nevtralen rezultat pri preverjanju (Listing 6.6). Takšno sporočilo se obravnava, kot da zapisa SPF sploh ne bi bilo.

Listing 6.6: Posredovanje sporočila s SPF.

```
Received-SPF: none (google.com: turk.alenka@guest.arnes.si does
    not designate permitted sender hosts)
    client-ip=2001:1470:8000::74;
Authentication-Results: mx.google.com;
spf=neutral (google.com: turk.alenka@guest.arnes.si does not
    designate permitted sender hosts)
    smtp.mail=turk.alenka@guest.arnes.si;
```

6.2 Testiranje mehanizma DKIM

Delovanje DKIM-podpisovanja odhodnih sporočil iz našega strežnika smo preverili s poslanim sporočilom. V izvornem sporočilu prejemnika smo opazili dodatno polje `DKIM-signature` (Listing 6.7). Če prejemnik preverja podpisovanje DKIM sporočil, so v polju `Authentication-results` vidni tudi rezultati preverjanja (Listing 6.8).

Listing 6.7: Polje »DKIM-signature« v glavi sporočila prejemnika.

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=snupi.si;
s=snmail; t=1409670682; r=y;
bh=YiPuor0x93cmcBI8kuym1+McHzXPUFUSXnjevNtEHlo=;
h=Date:From:To:Subject;
b=R1XPc/yk19jNGRwY0XyrCKC8+fhixq3BDpVrl9bKxmY/tzOBzVV2at3ej93Nl5/MA
MXYNqc9IHpNXWcT4WRtVde1FEY5MhBw7b9ZeRfPI/geD5HVt1t/j1C1L/X5bxOj/9D
yTbqBgp6T5IFGxD8q3+voTcBQX4hvZmcHreFolXY=
```

Listing 6.8: Polje »Authentication-results« z rezultati preverjanja.

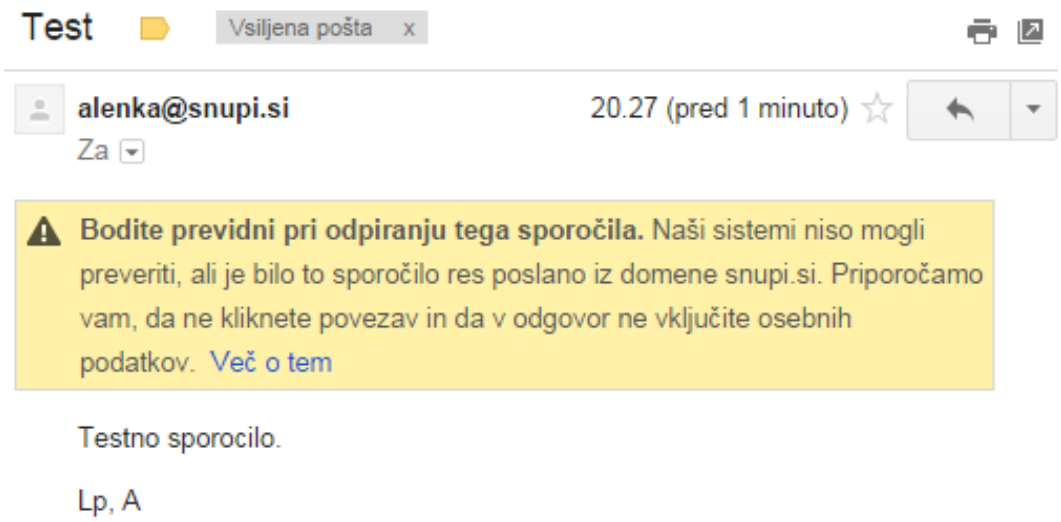
```
Authentication-Results: mx.google.com;
dkim=pass header.i=@snupi.si;
```

Testiranje smo pri DMARC mehanizmu izvedli na enak način, kot pri SPF. Pošiljali smo sporočila iz ne-avtoriziranega strežnika ter s spreminjanjem parametra `p=` v zapisu TXT preverjali ustreznost delovanja različnih načinov politik. Nobeno izmed prejetih sporočil ni bilo DKIM podpisanih, SPF pa je vračal neuspešno preverjanje naslova IP. Pri politiki `none` je bilo sporočilo dostavljeno v poštni predal prejemnika, glava prejetega sporočila pa je pokazala, da sicer rezultat preverjanja avtentikacije domene ni bil uspešen (Listing 6.9).

Listing 6.9: Rezultati preverjanja politike »none«.

```
Authentication-Results: mx.google.com;
spf=hardfail (google.com: domain of alenka@snupi.si does not
    designate 2001:1470:8000::74 as permitted sender)
    smtp.mail=alenka@snupi.si;
dmarc=fail (p=NONE dis=NONE) header.from=snupi.si
```

Sledilo je preverjanje politike `quarantine`. Poslano sporočilo je pri prejemniku končalo v mapi z neželeno pošto in ga hkrati opozarjalo, da to sporočilo morda ne prihaja od zaupanja vrednega vira. Podrobnosti so vidne na Sliki 6.1.



Slika 6.1: Prejeto sporočilo v Gmail z DMARC politiko `quarantine`.

Polja glave lahko analiziramo in preverimo poravnave identifikatorjev. Ker prejeto sporočilo nima podpisa DKIM, preverjamo le mehanizem SPF. V polju glave `Return-Path:` vidimo domeno pošiljatelja »snupi.si«. Primerjamo jo z domeno polja glave `From:`. Opazimo, da se domeni ujemata. Ker pa je preverjanje zapisa SPF ugotovilo ne-avtoriziran IP, je sporočilo neporavnano. Glava sporočila je prikazana v Listing 6.10.

Listing 6.10: Prejeto sporočilo z DMARC politiko »quarantine«.

```
Delivered-To: alenka.turk.13@gmail.com
Received: by 10.220.81.202 with SMTP id y10csp339827vck;
Tue, 9 Sep 2014 11:27:56 -0700 (PDT)
X-Received: by 10.180.24.35 with SMTP id
    r3mr31345598wif.71.1410287276267;
Tue, 09 Sep 2014 11:27:56 -0700 (PDT)
Return-Path: <alenka@snupi.si>
Received: from mail.arnes.si (axy.arnes.si. [2001:1470:8000::74])
by mx.google.com with ESMTPS id
    s1si18136086wju.151.2014.09.09.11.27.55
for <alenka.turk.13@gmail.com>
(version=TLSv1.2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
Tue, 09 Sep 2014 11:27:56 -0700 (PDT)
Received-SPF: fail (google.com: domain of alenka@snupi.si does not
    designate 2001:1470:8000::74 as permitted sender)
    client-ip=2001:1470:8000::74;
Authentication-Results: mx.google.com;
spf=hardfail (google.com: domain of alenka@snupi.si does not
    designate 2001:1470:8000::74 as permitted sender)
    smtp.mail=alenka@snupi.si;
dmarc=fail (p=QUARANTINE dis=QUARANTINE) header.from=snupi.si
Received: from axy.arnes.si (localhost [127.0.0.1])
by axy.arnes.si (Postfix) with ESMTP id 5B3357200E3
for <alenka.turk.13@gmail.com>; Tue, 9 Sep 2014 20:27:55 +0200
    (CEST)
Received: from mail.arnes.si ([127.0.0.1])(amavisd-new, port 10024)
with ESMTP id QEammSx54835 for <alenka.turk.13@gmail.com>;
Tue, 9 Sep 2014 20:27:55 +0200 (CEST)
Received: from xyz.arnes.si (xyz.arnes.si [193.2.1.177])
by avs1.arnes.si (Postfix) with SMTP id 47DC07202A8
for <alenka.turk.13@gmail.com>; Tue, 9 Sep 2014 20:27:24 +0200
    (CEST)
```

```
Subject: Test
Message-Id: <20140909182735.47DC07202A8@avs1.arnes.si>
Date: Tue, 9 Sep 2014 20:27:24 +0200 (CEST)
From: alenka@snupi.si

Testno sporocilo.

Lp, A
```

Politika `reject` je najstrožja in zavrne sporočilo, še preden je lahko dostavljeno v poštni predal uporabnika. Testiranje te politike je vrnilo ravno takšne rezultate. Na naslov `alenka@snupi.si` je bilo poslano obvestilo o zavrnjenem sporočilu.

S poslanim sporočilom iz lažno-predstavljenega naslova `alenka@mail.snupi.si`, vidnim v Listing 6.11, smo preverili, če implementirani mehanizem zavrača pod-domene. Medtem je bila določena politika `none`.

Listing 6.11: Sporočilo, poslano iz pod-domene »mail.snupi.si«.

```
220 mail.arnes.si ESMTP Postfix
MAIL FROM: alenka@mail.snupi.si
250 2.1.0 Ok
RCPT TO: alenka.turk.13@gmail.com
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Subject: Test
Testno sporocilo. Lp, A
.
250 2.0.0 Ok: queued as 20D27GH63L
```

Izkazalo se je, da je mehanizem pravilno ukrepal in zavrnil sporočilo, saj ni bilo dostavljeno v poštni predal prejemnika `alenka.turk.13@gmail.com`. Ker imamo sicer v veljavi tudi prejemanje na elektronski naslov s pod-domeno `mail.snupi.si`, smo v poštni predal uporabnika »alenka« prejeli sporočilo z obvestilom o neuspešni dostavi. Prikazano je na Sliki 6.2.

```
Reporting-MTA: dns; [illegible].arnes.si
X-Postfix-Queue-ID: CEC74720722
X-Postfix-Sender: rfc822; alenka@mail.snupi.si
Arrival-Date: Tue,  9 Sep 2014 20:32:02 +0200 (CEST)

Final-Recipient: rfc822; alenka.turk.13@gmail.com
Original-Recipient: rfc822;alenka.turk.13@gmail.com
Action: failed
Status: 5.7.1
Remote-MTA: dns; gmail-smtp-in.l.google.com
Diagnostic-Code: smtp; 550-5.7.1 Unauthenticated email from snupi.si is not
    accepted due to domain's 550-5.7.1 DMARC policy. Please contact
    administrator of snupi.si domain if this 550-5.7.1 was a legitimate mail.
    Please visit 550-5.7.1 http://support.google.com/mail/answer/2451690 to
    learn about DMARC 550 5.7.1 initiative. ev6si18110240wjb.171 - gsmtp
```

—ForwardedMessage.eml———————————————————————————

Zadeva: Test
Od: alenka@mail.snupi.si
Datum: 9.9.2014 20:31

```
Testno sporocilo.

Lp, A
```

Slika 6.2: Obvestilo o neuspešni dostavi, zavrnjena pod-domena.

Poglavje 7

Sklepne ugotovitve

V današnjem času, ko je elektronska pošta ena izmed temeljnih storitev v internetnem svetu, si ponudniki ne morejo privoščiti, da bi pri dostavi prišlo do zapletov zaradi pomanjkljivosti v protokolu SMTP. Uporaba naprednih overitvenih mehanizmov je nujna za zanesljivo delovanje. V diplomskem delu smo opisali pomanjkljivosti protokola SMTP in kako le-te odpraviti z uporabo dodatnih mehanizmov. Sledila je postavitev poštnega strežnika in namestitev ter testiranje teh mehanizmov.

Ugotovili smo, da je pošiljanje elektronske pošte z uporabo avtentikacijskih mehanizmov SPF, DKIM in DMARC resnično pripomoglo k prepoznavanju neželenih elektronskih sporočil in tudi k zanesljivi dostavi legitimnih elektronskih sporočil.

Z mehanizmom SPF smo v našem primeru določili le en avtoriziran naslov IP. Razlog temu je obseg našega testiranja. Če bi imeli več poštnih strežnikov ter gostovali storitev elektronske pošte z našo domeno na drugih strežnikih, bi temu ustrezno določili večje območje naslovov IP. S tem bi se povečala nevarnost zlorabe. S preverjanjem delovanja mehanizma smo v našem primeru ugotovili, da je uspešno zaznal ne-legitimno elektronsko pošto. Seveda je bil zaradi le enega naslova IP zapis za SPF precej preprost in se je izkazal za dokaj uspešnega. Ta mehanizem bi zato morali uporabljati vsi manjši ponudniki elektronske pošte, večji pa morajo biti pazljivi pri dodajanju avtoriziranih naslovov IP. SPF testiranje je pokazalo še, da ta način avtentikacije domene povsem neuporaben, kadar so sporočila posredovana iz drugih domenskih imen. To kaže na še večjo previdnost pri nastavljanju zapisa v DNS, saj si ne smemo dovoliti, da bi prišlo do zavrnitve

sicer veljavnega sporočila.

DKIM podpis sporočila se ohrani tudi pri posredovanju. Tukaj večji problem predstavlja sam algoritem podpisovanja, zaradi česar obstaja možnost da se na koncu izkaže za neveljavnega, čeprav gre za sicer legitimno sporočilo. To se lahko zgodi ob večkratnih posredovanjih tega sporočila med podpisujočimi strežniki SMTP. Že najmanjša sprememba glave sporočila lahko vodi v neuspešno preverjanje te metode. Zaradi te nevarnosti tudi nastavitev politike DKIM preverjanja ne sme biti preveč stroga. Lahko pa na ta način več lažnih sporočil roma v poštne predale uporabnikov. Pri uspešnem preverjanju načeloma nakazuje tudi na nespremenjeno vsebino sporočila, za bolj verodostojen dokaz pa se moramo obrniti na druge tehnologije z naslavljanjem zaščite vsebine sporočila.

Ker mehanizem DMARC združuje rezultate SPF in DKIM se je seveda izkazal za najbolj učinkovitega. Uspešno rešuje nekatere slabosti obeh mehanizmov. Četudi pride do posredovanja sporočila in je SPF tu neuporaben, lahko zaradi DKIM podpisanega sporočila, uspešno prestane test DMARC. DKIM izboljšuje predvsem s tem, da določa ukrepe DKIM nepodpisanih sporočil, brez da bi s tem zavrnil veljavna. Pomembna lastnost so poročila prejemnikov, ki nam pomagajo oblikovati politiko, najbolj primerno za naše uporabnike. Seznanjeni smo tudi s podatki, koliko ne-avtenticiranih sporočil je bilo poslanih z imenom naše domene in o kakšnih ukrepih bi bilo dobro razmisliti v nadaljnje. V primeru, da je zlorabljeno polje glave `Return-Path`, pa tudi DMARC ne more nedolžnih uporabnikov ubraniti pred ogromnimi količinami prejetih povratnih obvestil z neuspešno dostavo do elektronskih naslovov, kamor so neželena sporočila poslana v njihovem imenu. Zavedati se moramo tudi, da morajo biti ti avtentikacijski mehanizmi izvedeni s strani pošiljatelja in prejemnika v kolikor želimo, da se njihova uporaba obrestuje.

Naše testno okolje ni omogočalo obsežnega preverjanja posameznih mehanizmov. Za to bi potrebovali več strežnikov in večje število aktivnih uporabnikov naše storitve elektronske pošte, kar bi privedlo tudi do večje izpostavljenosti zlorabe našega poštnega sistema. Povečal bi se razpon prejemnikov, s čimer bi se srečali z več načini različnih konfiguracij tujih poštnih strežnikov, ki lahko vplivajo na prenos naše elektronske pošte. Potrebno bi bilo testirati več različnih načinov konfiguracij našega strežnika in temeljito preučiti rezultate vseh elementov zaščite. Vsak ponudnik elektronske pošte mora ukrepe izvajati glede na zahteve svojih upo-

rabnikov oz. rezultate preverjanja sporočil. Načini varnostnih mehanizmov se med seboj razlikujejo glede na to, katere elemente poštnega sistema želijo zaščititi. Zato je priporočeno, da se izkoristi čim več načinov za zaščito pred neželeno elektronsko pošto.

Naši implementaciji bi za resnejšo uporabo morali dodati dodatne tehnologije, ki izvajajo filtriranje in ocenjevanje na podlagi analize prejetih sporočil, še preden ti pridejo v poštne predale naših uporabnikov. Dodali bi lahko tudi preverjanje javnih seznamov črnih list, kjer najdemo znane pošiljatelje neželene pošte.

Dodatek

Zapisi virov v DNS

Zapis vira	domensko ime	vrednost
A	snupi.si	194.249.58.26
A	mail.snupi.si	194.249.58.26
MX	snupi.si	mail.snupi.si
PTR	194.249.58.26	mail.snupi.si

Tabela 7.1: Zapisi DNS za domeno snupi.si.

Konfiguracijske datoteke

Listing 7.1: Konfiguracijska datoteka Postfix, main.cf.

```
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
    194.249.58.0/26
mydestination = $myhostname, mail.snupi.si, $mydomain,
    localhost.$mydomain, localhost
inet_interfaces = all
smtpd_helo_required = yes
smtpd_helo_restrictions = permit_mynetworks,
    reject_invalid_helo_hostname, permit
smtpd_sender_restrictions = permit_mynetworks,
    reject_non_fqdn_sender, reject_unknown_sender_domain,
```

```
    reject_unauth_pipelining, permit
smtpd_recipient_restrictions = reject_unauth_pipelining,
    reject_non_fqdn_recipient, reject_unknown_recipient_domain,
    reject_unauth_destination, reject_unauth_destination,
    check_policy_service unix:private/policyd-spf,
    policyd-spf_time_limit = 3600 permit

smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth
smtpd_sasl_auth_enable = yes
smtpd_sasl_local_domain = snupi.si
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes

smtpd_tls_cert_file=/etc/pki/certs/mail.snupi.si.crt
smtpd_tls_key_file=/etc/pki/private/mail.snupi.si.key
smtpd_use_tls=yes
smtpd_tls_security_level=may
smtpd_tls_protocols= !SSLv2, !SSLv3

milter_dkim = inet:localhost:8891
milter_dmarc = inet:localhost:8893
milter_default_action = accept
milter_protocol = 2
smtpd_milters = $milter_dkim, $milter_dmarc
non_smtpd_milters = $milter_dkim, $milter_dmarc
```

Listing 7.2: Konfiguracijska datoteka Postfix, master.cf.

```
smtp      inet  n       -       -       -       -       smtpd -v
submission inet n       -       -       -       -       smtpd -v

policyd-spf unix -      n       n       -       0       spawn
user=policyd-spf argv=/usr/bin/policyd-spf
```

Listing 7.3: Konfiguracijska datoteka Dovecot, dovecot.conf.

```
protocols = imap imaps
disable_plaintext_auth = no
mail_location = mbox:~/mail:INBOX=/var/mail/%u

service auth {
unix_listener /var/spool/postfix/private/auth {
group = postfix
mode = 0660
user = postfix
}
}

ssl = required
ssl_cert = </etc/pki/certs/mail.snupi.si.crt
ssl_key = </etc/pki/private/mail.snupi.si.key
```

Listing 7.4: Konfiguracijska datoteka DKIM, opendkim.conf.

```
Domain              snupi.si
KeyFile             /etc/mail/dkim.key
Canonicalization    relaxed/simple
Selector            snmail
SignatureAlgorithm rsa-sha256
MinimumKeyBits      1024
```

Literatura

[1] P. M. Michael Adkins, "DMARC Training Series," MAAWG, Okt. 2012, dostopano: 10.6.2014. Na voljo na spletu: http://www.maawg.org/activities/training/dmarc-training-series

[2] S. Corporation, "Internet Security Threat Report 2014 :: Volume 19," Symantec Corporation, Apr. 2014, dostopano: 25.8.2014. Na voljo na spletu: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

[3] P. Resnick, "Internet Message Format," RFC 5322, IETF, Okt. 2008, dostopano: 8.8.2014. Na voljo na spletu: http://www.ietf.org/rfc/rfc5322.txt

[4] J. Klensin, "Simple Mail Transfer Protocol," RFC 5321, IETF, Okt. 2008, dostopano: 15.5.2014. Na voljo na spletu: http://www.ietf.org/rfc/rfc5321.txt

[5] Wikipedia, "Email," Jun. 2014, dostopano: 25.8.2014. Na voljo na spletu: http://en.wikipedia.org/wiki/Email

[6] ——, "MIME," Jun. 2014, dostopano: 12.9.2014. Na voljo na spletu: http://en.wikipedia.org/wiki/MIME

[7] M. B. in Tim Crosby, "How E-mail Works," howstuffworks.com, dostopano: 15.6.2014. Na voljo na spletu: http://computer.howstuffworks.com/e-mail-messaging/email.htm

[8] J. Klensin, N. Freed, M. Rose, E. Stefferud, and D. Crocker, "SMTP Service Extensions," RFC 1869, IETF, Nov. 1995, dostopano: 15.6.2014. Na voljo na spletu: http://www.ietf.org/rfc/rfc1869.txt

[9] R. Siemborski and A. Melnikov, "SMTP Service Extension for Authentication," RFC 4954, IETF, Jul. 2007, dostopano: 8.9.2014. Na voljo na spletu: http://www.ietf.org/rfc/rfc4954.txt

[10] A. Melnikov and K. Zeilenga, "Simple Authentication and Security Layer (SASL)," RFC 4422, IETF, Jun. 2006, dostopano: 8.9.2014. Na voljo na spletu: http://www.ietf.org/rfc/rfc4422.txt

[11] A. Freier, P. Karlton, and P. Kocher, "The Secure Sockets Layer (SSL) Protocol Version 3.0," RFC 6101, IETF, Avg. 2011, dostopano: 25.8.2014. Na voljo na spletu: http://www.ietf.org/rfc/rfc6101.txt

[12] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," RFC 5280, IETF, Maj 2008, dostopano: 12.9.2014. Na voljo na spletu: http://www.ietf.org/rfc/rfc5280.txt

[13] C. Adams, S. Farrell, T. Kause, and T. Mononen, "Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)," RFC 4210, IETF, Sep. 2005, dostopano: 12.9.2014. Na voljo na spletu: http://www.ietf.org/rfc/rfc4210.txt

[14] Kioskea, "How email works (MTA, MDA, MUA)," Kioskea.net, Jun. 2014, dostopano: 3.9.2014. Na voljo na spletu: http://en.kioskea.net/contents/116-how-email-works-mta-mda-mua

[15] T. F. D. Project, "Mail Components," FreeBSD, Sep. 2014, dostopano: 3.9.2014. Na voljo na spletu: https://www.freebsd.org/doc/handbook/mail-using.html

[16] R. Gellens and J. Klensin, "Message Submission for Mail," RFC 6409, IETF, Nov. 2011, dostopano: 8.9.2014. Na voljo na spletu: http://www.ietf.org/rfc/rfc6409.txt

[17] P. Documentation, "Postfix TLS Support," Postfix, dostopano: 15.6.2014. Na voljo na spletu: http://www.postfix.org/TLS_README.html

[18] J. Myers and M. Rose, "Post Office Protocol - Version 3," RFC 1939, IETF, Maj 1996, dostopano: 3.9.2014. Na voljo na spletu: http://www.ietf.org/rfc/rfc1939.txt

[19] M. Crispin, "INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1," RFC 3501, IETF, Mar. 2003, dostopano: 3.9.2014. Na voljo na spletu: http://www.ietf.org/rfc/rfc3501.txt

[20] R. Thurlow, "RPC: Remote Procedure Call Protocol Specification Version 2," RFC 5531, IETF, Maj 2009, dostopano: 12.9.2014. Na voljo na spletu: http://www.ietf.org/rfc/rfc5531.txt

[21] D. E. Jim McBee, "Mastering Microsoft Exchange Server 2010, strani 89-90, poglavje 3," Mar. 2010, dostopano: 12.9.2014.

[22] Wikipedia, "Simple Mail Transfer Protocol," Jun. 2014, dostopano: 15.6.2014. Na voljo na spletu: http://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol

[23] S. Kitterman, "Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1," RFC 7208, IETF, Apr. 2014, dostopano: 15.6.2014. Na voljo na spletu: http://www.ietf.org/rfc/rfc7208.txt

[24] D. Crocker, T. Hansen, and M. Kucherawy, "DomainKeys Identified Mail (DKIM) Signatures," RFC 6376, IETF, Sep. 2011, dostopano: 15.6.2014. Na voljo na spletu: http://www.ietf.org/rfc/rfc6376.txt

[25] Y. M. Kucherawy, E. Zwicky, "Domain-based Message Authentication, Reporting and Conformance (DMARC) draft-kucherawy-dmarc-base-04," Apr. 2014, dostopano: 10.6.2014. Na voljo na spletu: http://tools.ietf.org/pdf/draft-kucherawy-dmarc-base-04.pdf

[26] P. Mockapetris, "Domain names - concepts and facilities," RFC 1034, IETF, Nov. 1987, dostopano: 25.8.2014. Na voljo na spletu: http://www.ietf.org/rfc/rfc1034.txt

[27] ——, "Domain names - implementation and specification," RFC 1035, IETF, Nov. 1987, dostopano: 25.8.2014. Na voljo na spletu: http://www.ietf.org/rfc/rfc1035.txt

[28] P. A. Cricket Liu, "DNS and BIND, poglavje 2," Maj 2006, dostopano: 13.9.2014.

[29] R. Aitchison, "Pro DNS and BIND," Avg. 2005, dostopano: 14.9.2014.

[30] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, "DNS Security Introduction and Requirements," RFC 4033, IETF, Mar. 2005, dostopano: 25.8.2014. Na voljo na spletu: http://www.ietf.org/rfc/rfc4033.txt

[31] ——, "Resource Records for the DNS Security Extensions," RFC 4034, IETF, Mar. 2005, dostopano: 25.8.2014. Na voljo na spletu: http://www.ietf.org/rfc/rfc4034.txt

[32] ——, "Protocol Modifications for the DNS Security Extensions," RFC 4035, IETF, Mar. 2005, dostopano: 25.8.2014. Na voljo na spletu: http://www.ietf.org/rfc/rfc4035.txt

[33] Wikipedia, "Email authentication," Avg. 2014, dostopano: 5.9.2014. Na voljo na spletu: http://en.wikipedia.org/wiki/Email_authentication

[34] M. Libbey, "DKIM fights phishing and e-mail forgery," 2005, dostopano: 18.6.2014. Na voljo na spletu: http://www.ietf.org/rfc/rfc969.txt

[35] C. Janssen, "Canonicalization," Techopedia, dostopano: 15.9.2014. Na voljo na spletu: http://www.techopedia.com/definition/15646/canonicalization

[36] R. Aitchison, "Pro DNS and BIND 10," Feb. 2011, dostopano: 10.9.2014.

[37] M. K. Dave Crocker, "MAAWG DKIM Implementation Training Video," MAAWG, Feb. 2010, dostopano: 16.6.2014. Na voljo na spletu: http://www.maawg.org/activities/training/dkim-video-list